International Journal of Computational Intelligence Research
ISSN 0973-1873 Volume 13, Number 8 (2017), pp. 1871-1906

http://www.ripublication.com

Privilege Based Advance Halftone Secure Secret Sharing Scheme with Error Diffusion Technique Along with Adaptive Secure Confidential Key in the Visual Cryptography

I. Diana Judith
Research Scholar,
Department of Computer Science and Engineering,
Prist University, Vallam, Thanjavur-613403, Tamilnadu, India.

Dr. G.J Joyce Mary
Research Supervisor,
Department of Computer Science and Engineering,
Prist University, Vallam, Thanjavur-613403, Tamilnadu, India.

Abstract

In the area of medicine, storing medical images of the patient in a very secure manner becomes to be toughest challenge. As the development in the digitalization of medicine, medical images security becomes critical issues for providing the secure transmission of data and images over unsecured channels. To overcome such issues, visual cryptography has been introduced using cryptographic mechanism for secretly transmitted the data by splitting into secure shares along with its secret data/images which is stored with greater confidentiality but during the retrieving process of the secret images, it has higher chance of getting the data been hacked so still it remains as major concern in visual secret sharing schemes. Therefore, it is essential to make the secure shares in the appropriate manner so we propose Privilege Based Advance Halftone Secure Secret Sharing Scheme including Error Diffusion Technique along with Adaptive Secure Confidential Key using Diffie-Hellman Authentication Protocol.

At first, we make the significant shares which contain the secret data or images in the shares by providing privilege values to the specific participants in the proposed model. Then, visible input an image is translated into halftones

shares by using advanced halftone method along with error diffusion scheme. Later on, the secret medical image is spitted into advanced halftone shares having privilege value as well as significant image quality along with secret image. Finally, adaptive secure confidential key management based Diffie-Hellman authentication protocol is included with privilege value based shares for providing the highest security for the encrypting the medical images in the visual cryptography. Hence, the implementation values has demonstrated that the proposed model obtains effective performance in terms of the Peak Signal-To-Noise Ratio (PSNR), Mean Square Error (MSE) , Normalized Cross Correlation (NC), Structural Similarity Index (SSI), Error ration and execution time

Keywords: Privilege model, Advance Halftone Secure Secret Sharing Scheme, Error Diffusion Technique, Adaptive Secure Confidential Key and Diffie–Hellman authentication protocol.

I. INTRODUCTION

The medical images are generally stored in the digital media, so it is very essential to provide the secure access of medical images which becomes a major concern in digitalization era. In the current scenario, as the development in the digitalization of media, medical images security becomes critical issues for providing the secure transmission of data over unsecured channels. Images are often utilized in various domains such as online teaching, medical imaging and advertising, etc. In real- time application, for broadcasting the images through the internet and restoring on different platforms such as (hard- drive, cloud server, etc) [1]. The most common problem in securing the images are integrity, confidentiality and authenticity becomes a critical concern. The standard methodology in the medical data security furnishes guidelines and techniques to health care professional and entities to accomplish three elements in telemedicine security such as integrity, authenticity and confidentiality. The confidentiality requires to prevent the unethical access to the transmitting the medical images of the patients, whereas the authenticity and integrity services are required to confirm the ownership and identify tampering of the obtained images. The medical images would be bigger in size and larger in number, as it contains confidential data in the images [2]. Thus, two important aims are: (1) to protect the confidentiality and integrity of the patient's personal data and their medical images and (2) to provide the security for the greater extend in order to minimize the cost storage and enhance the speed of the data/ image transmission without affecting the image quality. Most of the information or data is replaced between any of the anonymous parties. Hence, it is very essential to utilize the encryption methods, whereas most preferable solution to protect the data as well as to provide the higher cryptography [3].

The secret data is revealed by the representing decryption process though applying the proper key. With limited time and computing facilities, it is difficult for attackers to decrypt n the confidential data by intends of statistical attack or exhaustive attack. The aim of computational security is obtained through the cryptography. The secret images can be exactly redeveloped by applying the Lagrange's interpolation. Even though such methods can give the distortion- free visual image quality in the redevelopment secret image, it requires a computing device to resolve the polynomials. The other generally approach is called as the visual cryptography, which was first introduced by the Naort and Shamir [4] in EuroCrypt. Inside this technique, a secret image is decayed into n useless shares which are further distributed n shares to the respondents. Decryption is potential by overlapping an adequate number (say, k) of shares.

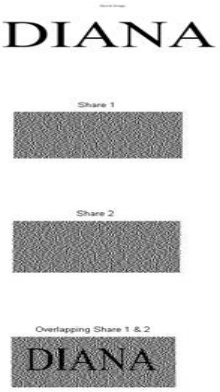

Fig.1 Visual scheme for binary images

Secret sharing mechanisms which safeguard and disturb a secret data or the images to the specific group of peoples provide solutions to the sharing issues. In this perspective, the fundamental example was first given by the Shamir and Blakley [5], have introduced new idea in the secret sharing scheme with threshold mechanism (t,n) which converts a secret information into n number of shares and distributes them to the desired respondents in a same manner that any t or larger number of shares can be accumulated to retrieve the secret data, but suppose t-1 any or fewer of them furnishes no data about the secret. Furthermore, to assure the retrieve the original secret data certain authentication techniques should be adopted so that any handling of shares is identified with greater probability ratio. To handle such issues, steganographic proficiencies are generally utilized [6]. In these mechanisms, first certain decent appearing images are utilized as cover images. Then the secret data or the information is combined into the cover image. Afterwards the secret information is merged with cover images and the outcome is stego types are distributed to the

desired participants by utilizing certain secret sharing mechanism. It clearly describes, to obtain the high quality stego images that should eliminate the suspicion nodes by using the secret sharing schemes. The most common method are steganographic schemes are utilized in steganographic secret sharing technique in which substitute least significant bits (LSBs) into modulus operation.

The technique in secret image sharing with steganography and authentication was introduced by Tsai and Lin in 2004. Their technique is an instance of a lossy polynomial-depend image sharing and the restored secret image would be distorted slightly.

According to the Wu.et al in 2004 [7] has introduced as another new mechanism in which the secret images are compressed at the beginning stage, and later on it was merged with cover images by utilizing the modulus operation. This mechanism can provide smaller stego based images, but the exact secret image would not be restored completely in the reconstruction procedures. To retrieve the secret images without any losses, this scheme was proposed by the author Lin and Thien [8], had utilized every pixel with certain value that splits more than two pixels with the value of 250. The hidden data is exposed by the corresponding decryption mechanisms with the appropriate the key. With the limited time and computing facilities, it is difficult for attackers to decrypt the confidential information of rigorous or statistical attack. The aim of the computational security has been accomplished through the security schemes.

The hidden data would be naturally exposed and should be decoded by the human visual system (HVS) without the use of any refined computation or any substitute algorithms. Furthermore, there is no detailed description about the sophisticated cryptographic mechanisms is required for the decryption and the encryption processes [9]. Nevertheless, the secret image would be inconspicuous if the number of stacked shares is minimum than k. This is termed as (k, n) threshold techniques. In spite of no exact encryption /decryption in visual cryptography, hereafter the process of image decay would still be termed as encryption and the progress of image stacking be called as decryption. Visual cryptography would be utilized not only in data hiding but also in various processes such as identification, authentication, access control, watermarking, key exchange etc.

Security analysis utilized in previous digital medical image systems are completed depend upon the traditional blocks ciphers such as International Data encryption algorithm, Advanced Encryption Standard and Data Encryption Standard. Nevertheless, because of the size of the data as well as image and enhancing demand for the real- time telereadiology and other various applications in online, these traditionally encryption algorithm would be preferable to obtain the higher security standard in hiding the image, moreover the delay in those approaches of Visual

cryptography. Therefore, to satisfy these difficulties and several of image encryption mechanism have been utilized.

To provide the advanced security in the visual cryptography, we propose Privilege Based Advance Halftone Secure Secret Sharing Scheme including Error Diffusion Technique along With Elliptic Curve Diffie–Hellman Encryption. At first, we make the significant share which contains the secret data or images in the shares by providing privilege values to the specific participants. Hence, privilege in the share are estimated in order to receive the secret images with privilege level in the advanced halftone secret sharing model along with the error diffusion techniques in order to avoid the noise in the secret medical images. Finally, Elliptic curve Diffie–Hellman algorithm is included with privilege value based shares for providing the highest security for the encrypting the medical images in the visual cryptography.

1.1 RELATED WORK

Blakey [10] et al had described about the two non parallel lines in the same plane where it intersect at particularly at one point. More commonly, any n dimensional hyper planes cross at a particular point. The secret sharing may be encrypted as any single element which coordinates, even though they are randomly selected, it has an insider in which the someone in possession of representing one or more of the n-dimensional hyper planes) that make secret data as it knows that which should lie on the same plane. In case the insider can obtain more knowledge about the secret data than an outsider would receive then the system will not have no longer data has theoretic analysis of the data security. If once only one of the n organizer node is utilized in which the insider understands clearly than any outsider (which means the secret data would be present in the X axis for the two dimensional system). Each user has provided with higher large number of data to determine the hyper plane; the secret image is retrieved by estimating the plane's point of intersection and therefore it is consuming the time for particular organizer to make the intersection. According to the Blakley' scheme, only less space is required than the Shamir's scheme, whereas Shamir's scheme each share required larger space for the exact secret images, in Blakley's method shares consumes t times larger, where t is depend on the threshold value of the users. Moreover, it is required to imply certain limitation on the usable shares on the dimensional planes. Final outcome is almost equivalent to the Shamir's polynomial system. Then later on author Monoth et al [11] had proposed a recursive visual cryptography with considering computationally complex in which it encodes the shares into numerous sub recursive shares. Simultaneously another author Kim et al [12] also endures from the computational complexity issues, even though it rejects dithering of the pixels. Later on analysis is carried out by the chetana Hedge [13] completely concentrated on post processing and the pre processing of the secret image

in order to obtain the quality images as the output and another method was proposed by the Van Tilorg[14] was depend upon the two important element such as contrast and pixel expansion.

Generally in visual cryptography, if shares generated in that image is merged and overlaid, but in most of the cases, the created share would not be a literal one and therefore the obtained result is a fake image so it is very important to protect such as malicious activity in the VC, author Tzeng et al [15] have proposed prevention scheme in order to avoid such fake images but there would not provided the authentication testing. A typical property of Visual Cryptography Scheme (VCS) was that can be visually, without any computational that decode the secret by superimposing shadow images. Nevertheless, majority of the contrast of the reconstructed images is only lost during the reconstruction process. A various kind of Visual Cryptography Scheme has been currently introduced by the Ching-Nung Yang [16], anticipated VCS with reversing scheme, permitting the respondents to do the reversing operation (reverse white and black) on the shadow images.

Ateniese et al. [17] had improvised visual cryptography that requires encryption for the hiding the secret data into number of meaningful shares. Generally, meaningful a logo message which is utilized for detecting the outer appears on the share. Hence, it is handling the meaningful shares in a flexible manner. Zhou et al. [18] had introduced scheme halftone visual cryptography to accomplish meaningful shares. The secret sharing images is encoded with desired size by applying both approaches such as improvised visual cryptography [16] and halftone visual cryptography [17] in which it is four times higher than those secret sharing images. To overcome this issues, Tsai et al [19] had represented a visual cryptography – based on visual secret sharing mechanism to produce the meaningful shares; in this mechanism, it had reduces the pixel expansion into two in order to obtain the greater meaningfulness shares. Therefore, lower pixel expansion was equated with proposed mechanism, represented in earlier studies. Even though the aforementioned visual secret sharing scheme can totally expose the true secret but still they would not accomplish the importance of the progressive image sharing, therefore, large number of shared images are overlaid which affects the quality of the retrieved secret images. According to the Jin et al [20] had represented the first progressive visual cryptography approach. Nevertheless, this approach suffers from the additional computational which breaches the important considerations in the visual secret sharing scheme VSS.

Later on Fang and Lin [21] has introduced another new method in the visual cryptography based progressive scheme, it does not needed any addition computation; However, it has one major drawback that is pixel expansion is very bigger than the other methods. To migitate pixel expansion, author Hou and Quan [22] had proposed the progressive visual cryptography with unexpanded meaningful shares. The

important aim of this scheme was to reconstruction without expanding the pixel size, the previous studies was already described about the progressive shares which is not user friendly in handling the meaningless shares. An advanced standard of security is included by adding a d forgery detection technique after executing the visual cryptography. The method we are utilizing for forgery detection is JPEG Ghost proficiency [22].Hence, the retrieved medical images experiences JPEG Ghost proficiency in order to detect the forgery in the medical images. In case, retrieved image is forged then the medical image would be rejected or else image can be accepted.

According to the Hwang et al [23] has proposed an image protection mechanism depends upon the computational integral mechanism, in which the 3D water mark information is merged into the DWT domain. By using computational integral imaging mechanism, it can retrieve the images in the 3D watermark scheme. This method is extremely robust due to the data redundancy of the primary images. Nevertheless, in the watermark extraction process, CIIR is a pixel superposition retrieving scheme. The apparent solution for the retrieving scheme in the #d plain image is significantly reduced as the increases in the magnification ratio.

According to the Piao et al [24] had described about the enhancement in the encryption technique for the image processing depend on the two important parameters pixel scrambling and the integral imaging scheme. In the retrieving process, the input image is developed by using CIIR scheme. This approach is highly robust and secure for the encryption scheme in the image processing system. Nevertheless, it includes resolution reduction issues.

Gao and Chen et al [25] had introduced the Huber- chaos scheme in the image encryption technique, which utilizes a normal plain image for the matrix permutation in order to shuffle the image pixel size and positions with regards of the logistic maps. Later on, the different stages compounding of hyper-chaos is utilized to exchange the gray values of the shuffled- image in terms of the diffusion process. Their method would not exists for the longer time duration in prevent the attackers.

Belghith and Rhouma et al [26] had introduced the unique key encryption mechanism to retrieve the images. The author has successfully introduced new technique to retrieve the ciphered image without any knowledge on any key value in the cryptosystem by utilizing the selected cipher-text attack and selected plain- text attack.

Zeghid et al [27] had demonstrated about the current advanced version of the AES which process with the design analysis of a secure symmetric image encryption method. The advanced encryption standard (AES) is redeveloped to advance an image encryption in the key stream generator to overcome the issues in the textured zones which lies in the another well encryption algorithms. The major issues in the

advanced encryption standard algorithm was totally depend upon the creation of the repetitive spatial rules, sensitive to the input image, time complexity and overall computational . In the region of data hiding in certain steganographic based applications favor to utilize the traditionally pseudo-random number generator method which grade the requirement and basic element for any stochastic simulation process in which the proposed system utilize the deterministic algorithm with random objects and random variables.

Author LeinHarn et al [28] had proposed Group Authentication scheme particularly developed for the security purpose in the group based applications. At first, it authenticates all the users at once and gives multiple authentication to the users. In this concept, they utilize the group administrator to take in charge of all the activities of the group member and it main function is to register all the group members as well as provide a secret token for each time. The author utilizes both the asynchronous and synchronous group authentication mechanism with (t, m, n) scheme , where t is represented as threshold value, m is represented as number of users and finally n is represented as the number of group members. The proposed method is depend on the shamir's secret sharing technique (t, n) and their asynchronous scheme uses (t, m, n) as secret sharing approach with single time authentication process and whereas another method is defined as the GAS with multiple level authentication technique. The group authentication protocol permits each user to reuse their secret tokens that leads to the decrease in the security.

According to the author Sian Jheng et al [29] had proposed dynamic group authentication scheme in the Visual cryptography. Their approach is similar to probabilistic model, it adopt dynamical change of users in the group, i.e. it can dynamically include multiple users or eliminate them from the user group. The proposed visual cryptography scheme A(t, n) with unlimited n is aimed to minimize the key generation overhead and broadcasting the transparencies. Therefore, a (t,∞) is included in the visual cryptography method to obtain highest contrast. This method is depend on the basis matrices, it cannot be developed with infinite size

According to the IlkerNadiBozkurt et al [30] has described about the Threshold Cryptography depend on the Blakley's Secret Sharing mechanism. Threshold Cryptography is performed with Blakley's and represent a RSA cryptosystem for the function sharing method. In existing Blakley's Secret Sharing method uses two both share combining and dealing phase. The essential values for the each computation are distributed to the trusted parties with the help of secret sharing technique. This methodology is depend on the intersection point and hyper plane geometry in order to produce the secret value.

According to the Ta-Wen et al [31] had performed on the neural network approach in the visual cryptography, In their method, a novel method for the visual cryptography

applying neural network technique. To execute encrypting method, gray level images are taken as the input and set of binary images is obtained as the output images. In this work, for converting input images from gray to binary, it is uses the image half toning technique. Moreover, the Quantum Neural Network for (2, 2) method is derived from the neutral network. It reduces the energy variable of a Quantum Neural Network for resolving the issues without utilizing any noise reduction technique.

SmitaJhajhariaet al [32] et al had proposed genetic algorithm in public key cryptography by applying neural network. They utilized public key cryptosystem for key generation by the application of artificial neutral network along with genetic algorithm. In this work, genetic algorithm is utilized for solving the search issues with the help of public key cryptosystem that produces pseudo random number to generate unique secret key and random key is applied in the artificial neural network, which obtains the results from the feed forward neural network.

Liu et al [33] had discussed about the robust readable H.264/AVC method for the secret information hiding method without considering any intra-frame deformation drift in the technique. At the beginning of the process, it separates the real embedded information into various class by applying the secret sharing method. After that, they considered the BCH syndrome code (BCH code) method to encrypt the secret information for each class with the information. At last, they include the encrypted information using the Discrete Cosine Transform for the paired-coefficients, each class contains their selected frames which satisfies normal criteria to avoid the deformation drift.

Lee and Tsai et al [34] had proposed an advanced technique in the secret data hiding scheme through the PNG images depend on the secret sharing method of the Shamir's (k,n)-threshold. Wei et al. [35] had represented novel data hiding technique especially designed for the color images depend on the mechanism of XOR operation and visual cryptography. Three unique methods were represented such as binary, meaningful, shares and noise. Their proposed approach a has been developed from true color ranging from 256 colors to 65,536 images by extending the size of the clocks 3×3 to 5×5.

1.2 CONTRIBUTIONS

The major contributions of this paper is provide the security the medial images, in order to share the images secretly, large number of algorithms and techniques has been proposed but selection of the image is based upon the quality of the images and the number of shares going to be created. Quality of the image is not the same when the shares are merged again. A single technique or a method does not provide quality image and acknowledgement of the shares sent. Furthermore, there is no privilege is given for the shares for retrieving process . Hence we motivated to work on

improving the quality of the image and confirmation of the image sent to the particular person through the adaptive secure confidential keyDiffie Hellman authentication protocol along with privilege model for retrieving images based advance halftone secure secret sharing scheme with Error Diffusion technique.

II. PRELIMINARIES

In this section, we analyze on preliminaries of the elliptic curve cryptography (Vankamamidi et al [43]) for potential terms to be accepted before describing into the proposed system

2.1 ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptography (ECC) is an another solution for the Public Key cryptography. It is depend upon the algebraic calculation of the elliptic curves over finite points. It considers p as a prime number and F_p as finite field. Generally, elliptic curve E is determined as a non singular curve that is mentioned in the common equation $Y^2 = x^3 + ax + b$, where a, $b \in F_p$ are defined as arbitrary constants which meeting the $4a^3 + 27b^2 \neq 0$. A any pair of (x, y), where x, $y \in F_p$, is specific points on the cure that can meet the requirement of the above equation. Hence, the elliptic curve points of (x_1, y_1) and (x_2, y_2) are used for the point addition in order to generate the third point in the curve. The elliptic group theory contains the group operation performances with set of points (x_2, y_2) to the actual point of the curve for making the abeliangroup with the center point O represents as identity element. Therefore the elliptic curve forms certain special features that prepare themselves essential for security applications [34].

In any cryptographic mechanism utilizing ECC, all the respondents parties should accepts the fundamental elements which defining the domain parameters in the elliptic curves. If the p is defined as the prime number in the field whereas the and f is defined as the binary case.

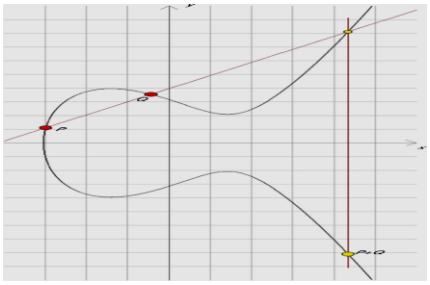

Fig. 3. Elliptic addition of two points on the curve

The cyclic subgroup a of $E(F_p)$ is determined by its key generator P and order n, it called as base point. The public domain parameters considered in the elliptic curve are p as the prime and a, b are determined as constants and order n in the fields points. The secret private key is randomly selected from the integer s with uniformly in range of $[1,n]$, whereas the corresponding the public key is estimated by $Q=[s]\times P$. The diffie key exchange problem is also an very important scheme in providing the security in the Elliptic curve cryptography mechanism, as it tend to be the toughest problem in the mathematically calculations, so we adopt double point scalar multiplication to generate the private key for the diffie key exchange mechanism, it is described in this below section.

2.2 COMPUTATIONAL PROBLEM

In this subsection, we review some of the older computations issues lies on the elliptic curve group. We propose a novel method to produce the adaptive secure confidential key management based on diffie-hellman authentication protocol**.**

2.2.1 DEFINITION1

It describes about the elliptic curve discrete logarithm problem. In the given tuple $(P,Q)\in G_p$, it is computing problem due to the polynomial- time bounded algorithm to discover an integer $k\in[1,n-1]$ such that $Q=kP$ [refer]

2.2.2 DEFINITION 2

It describes about the Computational Diffie-Hellman Problem. In a given tuple as $(P,a\bullet P,b\bullet P)\in G_p$ for any $a,b\in[1,n-1]$, computation of $a\bullet b\bullet P$ is tough for polynomial- time bonded algorithm.

2.2.3 DEFINITION 3

It describes about the elliptic curve factorization problem. In a given tuple, $(P,Q)\in G_p$, where $Q=aP+bP$ and $a,b\in[1,n-1]$. Computation of aP and bP are tough by a polynomial-time bounded algorithms.

2.3 BILINEAR PAIRINGS

Let G_1 indicates an additive set of prime order q, G_2 is a multiplicative group of the same order and P is a source of G_1. Additionally, let $\hat{e}:G_1\times G_2\to G_2$ is an permissible

mapping, which fulfills the following properties.

- **Bilinearity**: For any P, Q, R $\in G_1$ then we have $\hat{e}(P+Q,R)=\hat{e}(P,R).\hat{e}(Q,R)$ and $\hat{e}(P,Q+R)=\hat{e}(P,Q).\hat{e}(P,R)$.

  Hence , for any and $a,b\in Z_q^*:\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}=\hat{e}(abP,Q)=\hat{e}(P,abQ)$ holds.

- **Non-degenerate**: $\hat{e}(P,P)\neq 1_{G_2}$, where 1_{G_2} represents to be the identity element of the group G_2.

- **Computability:** There is an significant algorithm to calculate $\hat{e}(P,Q)$ for any P,Q$\in G_1$.

In common, G_1 is set of points on an elliptic curve, and G_2 is referred for multiplicative group of finite field. From this analysis, it is understood that map $\hat{e}$ would be obtained from the Tate pairing or enhanced Weil pairing over a finite field. For more comprehensive analysis about bilinear pairings and elliptic curves to choose a approximate parameters can be determined from (Vankamamidi et al [43]) for improving the security and efficiency.

2.4 ELLIPTIC CURVE DIFFIE-HELLMAN ALGORITHM

As this Elliptic Curve Diffie-Hellman algorithm is much better than the existing method like RSA (Rivest-Shamir-Adleman) algorithm, because ECDHA (Elliptic Curve Diffie-Hellman algorithm) needs the key exchange protocol between the two parties in order to securely transmit the data or the images which gives the exact forward secrecy. If data or images requires to be transmitted between the various parties, each party can obtain the secret keys on the same curve and, therefore it provides unique key as the public and secret key pairs to transmit or exchange the data or images between the parties, which is not possible in the RSA encryption. Hence, we have described the Diffie- Hellman algorithm in the step by step process, which is given below:

2.4.1 PROCEDURE FOR THE KEY GENERATION

- The Diffie- Hellman algorithm needs two highest numbers such as prime (*n*), and (*g*), a primitive root of *n*
- Next, choose any two secret values *a* and*b.*

- Equate common public values x' and y'.
- $x' = ga \bmod n$
- $y' = gb \bmod n$
- Then, exchange the public values x' and y'
- Next, Equated secret value is shared
- $ka = ya \bmod n$
- $kb = xb \bmod n$

From mathematically analysis, we determine that $ka = kb$, hence, Diffie- Hellman algorithm is described.

III. RESEARCH METHODOLOGY

In this research, we propose the Privilege Based Advance Halftone Secure Secret Sharing Scheme including Error Diffusion Technique along With Adaptive Secure Confidential Key Using Diffie-Hellman Authentication Protocol. The proposed system provides the highest security for the encrypting the medical images in the visual cryptography. The secure visual quality of secret images by privilege based advanced halftone scheme including diffusion techniques with adaptive secure confidential key using Diffie-Hellman Authentication Protocol. At first, the visible input images is translated into halftones shares by using advanced halftone method along with error diffusion scheme. Later on, the secret medical image is spitted into advanced halftone shares having significant image quality along with secret image in it. Here, the shared images from the advanced halftoningprocess are distributed to the targeted participants and moreover, it is heavily forced to expose the secret images. When the shares are produced, it is applies the advanced halftone processing. Then, images are encoded with high quality secret images by using the error diffusion methodology in order to provide the higher security. It uses Diffie–Hellman authentication protocol for encryption and then decryption the secret images with same image quality by using diffusion methodology including Privilege model for secret sharing medical images.

In our method, we design the privilege model for secret sharing medical images with advanced halftoning process to make the significant shares, which contains the secret data or images in the shares. It provides the privilege values to the specific participants and the model is designed with different privilege values. When the specific participant has the higher privilege value then it has greater chance of retrieving the image, or else , it has lower privilege value and lower chance of retrieving the images for the specific participants. The proposed system for privilege analysis design is described in upcoming section. Moreover to reduce the error in the images as well as to improve the image quality, we use the error technology. Furthermore, we propose the reversible data hiding algorithm in the privilege model

for the improving the performance in terms of the PSNR (Peak Signal to Noise Ratio), Error ratio and the execution time considering the encryption time.

3.1 PRIVILEGE-BASED ADVANCE HALFTONE SECRET SHARING MODEL

We analysis the process visual cryptography for the Privilege-Based Advance Halftone Secret Sharing Model. At first, the steps for reconstructing the secret medical images have undergone the superimposition of the generated shares. This activities is almost relevant to bit level of OR operation utilized in the logic metric operation. While the large number of shares are stacked, whereas the pixels in the tacked secret image would be turned as black (1) when any share contains the black pixel at any location in the images. The pixels would look white (0) when all the shares are remains to be in white in pixels in any location. Later on, the human visual system generally concentrates on the binary image, especially on the darker side of the image. Therefore, white part will be neglected for back ground. Consequently, when a share contains of larger number of black spots for decrypting process, it can disclose the secret image at very faster rate, so we illustrate that this particular share has given the top privilege. On the another term, when a share has lesser black spots and adds certain contrast development in the retrieved image, which has lesser privilege. Hence, we adopt the probability of black shares to introduce the new shares with various significance levels.

Let us consider privilege range of respondents $R_{PL_i}, i = 1,....,n$ without loss of generalization, we frame $R_{PL_i} = i$, which means $R_{PL_i} > R_{PL_{\hat{i}}}$ for $i > \hat{i}$. In this summation, two $n \times m$ sharing matrices C^0 and C^1 are developed to discharge the black and white shares for the privilege based shares, respectively. In C0 and C1, where each column in the matrix represents the vector thatshares from one to m ways with the influenced random number in the matrix. Every row vector demonstrates about the pixel values is apportioned from one of n respondents. It is mentioned that column C0 and C1 has the number of blacks spots (1s) which is larger than the i^{th} row. It represents that row $i > 1$ is demonstrated that without including the loss of the generalization, where the element i is apportioned to share RS^i. Hence, respondents i consider more quantity of black spots which produces higher privilege than participants $\hat{i}$, where $i > \hat{i}$

3.1.1 DESIGN ANALYSIS OF THE PRIVILEGE MODEL

In the design analysis of the sharing matrices are explained below, it is indicates that all the columns and rows are considered from 1. At first, we design first columns in the matrix C^0, in which it classified into right CR^0 and left side is CL^0 in the matrix. In CL^0, there have $n-i$ whites (0) in the *ith* row and here 0 s in those matrix are all apportioned to various columns. Thus, CL^0 requires at least $m_1 = \sum_{i=1}^{n}(n-i) = n(n-1)/2$ columns to store the 0s , and then overall size of the columns left side will be represented as $n \times m_1$. On the other side, the rest of the attributes in the columns left side CL^0 are completely filled by the 1s i.e. black spots. Let A_i consider the number of 1s to seem in the *ith* row of CL^0 (i.e. CL_i^0). Afterwards, $A_i = m_1 - (n-i) = (n^2 - 3n + 2i)/2$. A_i will gain as i finds bigger. Therefore, the possibility of the black spots shares are based on the respondents privilege level i from any of the shares RS^i. Hence, it is estimated the parameters of m_1 and A_i

$$m_1 = n(n-1)/2 \tag{1}$$

$$A_i = (n^2 - 3n + 2i)/2 \tag{2}$$

Then, we design the C^1: To improve the security in each shares, we adopt the adaptive secure confidential key using elliptic curve diffie key authentication protocol for making the share, in the *ith* row of C^1 (which is given as C_i^1) it should remain as similar as the CL_i^0, that is almost equal to $(n^2 - 3n + 2i)/2$.

However, to enhance of the privilege in the stacked shares. We adjust all the 1s to the various columns. The rest of the elements in the C^1 are all set to 0. Hence, the size of the C^1 is the $n \times m$, where $m = \sum_{i=1}^{n}(n^2 - 3n + 2i)/2 = n(n-1)^2/2$. From the design analysis of the parameter m is given as

$$m = n(n-1)^2/2 \tag{3}$$

While designing column of the right side of CR^0, it is stated that size of the C^0 and C^1 must be the similar. As to have the same chance of having black shares with or without considering the security features in the shares. Therefore the result in the column of right side $C^0(CR^0)$ is represented as $n \times m_2$, where the following criteria is given as $m_2 = m - m_1 = n(n-1)^2/2 - n(n-1)/2$, it is finally given as $n(n-1)(n-2)/2$. The attributes in

the column right side is CR^0 are adjust to 0. The design analysis of the parameter m_2 is given as

$$m_2 = n(n-1)(n-2)/2 \tag{4}$$

For the enhancing the security, the ith row in C^0 and C^1 have the similar value of the A_i, which is represented as "1" . This clearly indicates that any share will have their privilege value i, whether the secret region is black or white spots. The chances of getting highest probabilities of black spots in the image (1) when the share RS^i is similar as $\beta_i = A_i / m$. As share RS^i has the same average light transmission $(1-\beta_i)$ for the both secret black spots and the white regions. Moreover, it does not provide any details or information about the secret image as it is securely encrypted in the process. Since the content of the share is fixed by the random number, the distribution of the white and black pixels will be haphazardly disordered. Hence, the sketch of the secret image will not reveal in the share. As the outcome, the share is considered as the secure.

Once the privilege model is designed is combined with Advanced halftone secret sharing scheme. In this section advanced halftone image is received by implementing error diffusion halftone scheme on a grey scale image G or any color image, This proposed model would use the secret image pixel at a moment and one column as well as row at a moment. The present pixel is compared with the threshold value (127.5). When the current pixel is higher than the threshold value, then would produce the white pixel as the final outcome image. When the pixel is much lower than the threshold value, then it produce the black pixel. When the pixel stays to the exact to threshold value then it can used for the color image. Hence, it is based on the threshold value to decide whether the produced pixel would be full black or full white or color image for the secret image. In this method, we take the advance halftone images which is obtained from above threshold value method for considering to the respondent one. Thus complementary image $I^{'}$ is obtained by reversing all white/black pixels of I to black /white of $I^{'}$ or sometimes even color image is included, which have been distributed to respondents 2 . Finally, privilege in the share are estimated in order to receive the secret images with privilege level in the advanced halftone secret sharing model along with the error diffusion techniques in order to avoid the noise in the secret medical images.

3.2ERROR DIFFUSION TECHNIQUES IN THE PRIVILEGE BASED ADVANCED HALFTONE SECRET SHARING MODEL

In this privilege model, we include the advanced halftoning process along error diffusion method for the secret medical images from the sender to receiver. It applies

non causal error filter of 5×5 of the error diffusion method. In this method, it diffuses the error in the privilege pixels, where the error is estimated from the difference between the original image value and the reconstructed image value. Let I be the generalized $M\times N$ image. For the present pixel be (a,b), $1\le a\le M$, $1\le b\le N$, $Q(a,b)$ is its predefined threshold value, $I^{'}(a,b)$ is its defined advanced haftone value. In this mechanism, it include error diffusion matrix , where as the error is represented as $E(a,b)$. Hereby, it uses the Floyd-steinberg error diffusion matrix with global threshold vale [0.5]are included in this method.

In common, each pixel is used the low pass filter in the quantization error method and then it is provided as the feedback mechanism for the next input samples to reduce the noise error. It is clearly represented in the Fig.2, which explains using the pictorial representation of the error diffusion method.

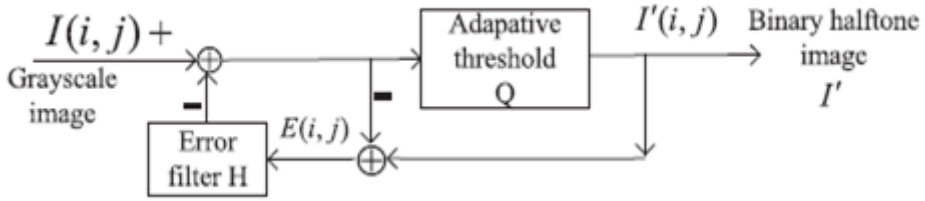

Fig .2 Error Diffusion Method

3.2.1 STANDARD ADAPATIVE THRESHOLD

The standard adaptive threshold value merges the important features of the computational level and the image pixels . It is estimated as follows:

The histogram of the I is generalized by utilizing equation (5) . The given equation (5), T is considered as the overall number of pixels in the I, Quantization error, T_Q is the total number of pixels which is associated with r_Q and finally L represented as the input grayscale images levels in I.

$$P_r(r_Q)=\frac{T_Q}{T},\ Q=0,1,2,.....,L-1 \tag{5}$$

Consider the threshold value is 0.5, Gray scale images and pixels are taken as D_0 with the value of $[0,1,.....,Q-1]$. Whereas the grayscale images and pixels of range $[Q,Q+1,.....,L-1]$ is denoted as D_1. Select Q that enlarges inter-class gap from D_0 and D_1, this variance id defined as the standard threshold value globally. The inter

class is determined in the equation in (6)

$$Q= \arg\max(\sigma_B^2 = \omega_0(\mu_0 - \mu_T)^2 + \omega_1(\mu_1 - \mu_T)^2) \quad (6)$$

Where

$$\omega_0 = \sum_{q=0}^{Q-1} P_q(r_q), \qquad \omega_1 = \sum_{q=k}^{Q-1} P_q(r_q)$$

$$\mu_0 = \sum_{q=0}^{Q-1} qp_q(r_q)/\omega_0, \qquad \mu_1 = \sum_{q=Q}^{L-1} qp_q(r_q)/\omega_1,$$

$$\mu_T = \sum_{q=0}^{L-1} qp_q(r_q)$$

3.2.2 ERROR QUANTIZATION

The error quantization is represented in the equation (7)

$$I'^{(a,b)} = \begin{cases} 1, & if I(a,b) \geq Q \\ 0, & if I(a,b) < Q \end{cases} \quad 1 \leq a \leq M \text{ , } 1 \leq b \leq N \quad (7)$$

If the standard threshold is taken for determining the value of the quantization error. Actually, the pixel value of the I(a,b) is quantized from the range [0,1] to value 1 or 0, it represents 1 for the white pixels and 0 for the black a pixels.

3.2.3 ERROR COMPUTATION

$$E(a,b) = I(a,b) - I'(a,b) \quad (8)$$

3.2.3 ERROR DIFFUSION MATRIX

$$\begin{bmatrix} 0 & (a,b) & 7/16 \\ 3/16 & 5/16 & 1/16 \end{bmatrix} \quad (9)$$

Form the error diffusion matrix is represented as present pixel location. The coefficients in the four direction indicates the amount of ratio occurred in the error occurred into all these four corners. It is potential possibly to accomplish the reconstructed image without noise using the error diffusion method and the overall quality of the input images as well as security images have been higher. In order to obtain the quality from the reconstructed images, repeat the process of error

quantization, computation and error diffusion matrix.

In this grayscale images or other input images is indicated as $n(n \geq 2, n \in Z^{+})$, the binary secret images is referred as S^{0} with pixel value of the secret image is given as $S^{0}(a,b), 1 \leq a \leq M, 1 \leq b \leq N$. The cover images hides the secret image after the creation of shares are represented as SS_{p} . The reconstructed secret image from $(2 \leq k \leq n, k \in Z^{+})$ cover images are referred as $S^{'}$.

Therefore, error quantization of the low pass filter is applied and it is shifted into next neighborhood pixels. The error filter is represented as FIR with the coefficient at (0,0)=0. The error filter are commonly considered as low pass filter in order to reduce the noise level using error diffusion matrix. It is connected to the advance halftoning process in order to provide the feedback response mechanism of the error report, considered to the input images in this mechanism for handling the sharp edges in the images. Hence, the proposed method with error diffusion matrix to reduce the error by minimizing the difference between the original image and reconstructed images. It is distributed in the complete process for making the secure image transmission using the visual cryptography

3.2.4 ADAVNCED HALFTONING PROCESS

In this method, it uses the advanced halftone image I is obtained from the error diffusion matrix m mechanism on a color image or on a grey scale image. It involves in the creation of privilege based shares using fundamental visual (2,2) scheme which applies both input advance halftone image as well as the advance secret image. We include reconstruction mechanism to retrieve the images from all the shares present in the halftone. Advance haftoningprocess has important process such as advanced encryption process and advance decryption process. In this encryption scheme, it uses the privilege base shares are obtained from the basic (2,2) visual mechanism. The information of the secret medical images are first encoded into halftone image I and the complementary halftone image is represented earlier as I'.

To encode the secret medical images is referred as p into a $Q1 \times Q2$ halftone matrix, it comprises of privilege share for each pixel. When it required only two pixels then it is denoted as secret image pixels, therefore, it is very essential to change the halftone cell. The secret data sharing must contain two pixel of secret data which should present in same location in two secret image shares. Hence, as far as their image positions are not concerned with secret data creation. It satisfies the condition of the security requirement to enhance the visual cryptography. For making the effortless choice of selecting the secret data pixels, we use random selection mechanism in the halftone image. Once after the encryption process, it very essential to make decode

the secret data pixels based privilege shares. The secret data pixels are embedded in the proposed methods are reconstructed from the shares which has been obtained in encryption method are stacked on each other shares. Finally, all the shares are superimposed that vanishes the effective data and produce the secret data through retrieving process, it is discussed in the below section in the visual cryptography

3.2.5RETRIEVING PROCESS

In this step, it is designed for retrieving or reconstructing the original image considering the privilege shares and recollecting the entire huffed shares altogether. Next, these distributed privilege shares would obtain the original data with secret image without reducing its image quality. This secret medical image would be used for building the significant and secure transmission of the data or images; the adaptive secure confidential key using diffie-hellman based authentication protocol is applied here to provide higher image as well as data security

3.3SELECTION OF ADPATIVE SECURE CONFIDENTIAL KEY FROM THE DIFFIE–HELLMAN AUTHENTICATION PROTOCOL

Once after, error diffusion techniques is applied in the privilege based advanced halftoning process, then adaptive secure confidential key from the diffie-hell man authentication protocol is applied. In this section, it deals with analysis of diffie key based authentication protocol. It provides adaptive secure confidential key exchange in order to transmit the secret medical image from sender to receiver by using Elliptic curve based diffie-hell man authentication protocol in the privilege based advanced halftoning model.

3.3.1ECC- DOUBLE SCALAR MULTIPLICATION

In ECCdouble scalar multiplication is utilized for making double point addition and multiplication, which considers the followings points P_0, P_1 for the addition point in the third point of EC $P_2(P_2 = P_0 + P_1)$. In double point addition is represented as $P_3(P_3 = 2P_1)$. Here point multiplication is used for addition operation in any EC point P to itself e times (e is referred as PM scalar and e is expressed in terms of $e \in GF(2^k))$ to find an EC point $Q(Q = e.P)$ and can be moldered to a set of double point scalar addition algorithm or Montgomery power ladder (MPL).

In the two dimensional affine plane has the EC points in the (x, y) planes with coordinates points of x,y$\in GF(2^k)$ [43]. $GF(2^k)$ is considered as series of operation like point addition, subtraction, division and multiplication. We uses the flexible

multiplier $GF(2^m)$ that can be utilized for all $GF(2^k)$ marked over any k-degree irreducible polynomial, where $k \le m$. The most significant bit of serial multiplier of $GF(2^k)$ is k-th bit used as flexible serial bit. In case, if any bits does not have any true value (as $k \le m$) in the above process, we appoint padding functionality by satisfying those bites with zeros, which in turn called as zero padding . Therefore, process of zero padding is acquainted and explained as follows .If a $GF(2^k)$ variable is represented in $A(x) = \sum_{j=0}^{k-1} a_j \bullet x^j$ should be enrolled as an m-bit input $I(x) = \sum_{j=0}^{mk-1} i_j \bullet x^j$ on a flexible $GF(2^m)$ multiplier and then it should be transformed into $A_I(x) = \sum_{j=m-k}^{m-1} a_{j-m+K} \bullet x^j + \sum_{j=0}^{m-k-1} 0 \bullet x^j$. Apart from flexibility, $GF(2^k)$ obtains minimum critical part delay and hence it can accomplish higher flexible in delay.

3.3.6 ADAPTIVE SECURE CONFIDENTIAL KEY MANAGEMENT BASED ON DIFFIE-HELLMAN AUTHENTICATION PROTOCOL

In this subsection, we propose an adaptive secure confidential key management based on diffie-hellman authentication protocol, to generate a confidential key in the privilege share. The proposed analysis is depends on the following sections:

3.3.6.1 SET UP PHASE

It invokes sender S_i and make register to the remote server and at the initialization stage S_i receives the adaptive secure confidential key which is placed in the secret image of the privilege shares model. The upcoming process are accomplished to finish this process:

The sender S_i, and receiver R_i are perform the following process:

Here, h(.) belongs two –way hash function , || string concatenation and $\oplus$ denotes an exclusive operation.

(1) Sender S_i gets selects EC- points from the $GF(2^k)$ to choose X

(2) Sender S_i sends the secure confidential key SCK_i in the privilege model to get the request from the Diffie-Hellman based authentication protocol.

(3) S_i sends the (X|| SCK_i) to the Diffie-Hellman based authentication protocol

(4) S_i computes $g^x = h(X \oplus SCK_i)$

(5) Senders sends the session key SK_i to authentication key $AK_i = h(X \oplus SCK_i) \bullet SK_i$

(6) After S_i obtaining his own public key $g^{x'} = \text{mod}\, AK_i$ from diffie- Hellman authentication protocol

(7) Receiver R_j gets selects EC- points from the $GF(2^k)$ to choose Y

(8) Receiver R_j generates is secure confidential key SCK_j

(9) R_j sends the (Y|| SCK_j) to the Diffie-Hellman based authentication protocol

(10) R_j computes $g^y = h(Y \oplus SCK_j)$

(11) Receiver sends the session key SK_i to authentication key $AK_j = h(Y \oplus SCK_j) \bullet SK_j$

(12) After R_i obtaining his own public key $g^{y'} = \text{mod}\ AK_j$ from diffie- Hellman authentication protocol,

(13) Then, exchange the public values $g^{x'}$ and $g^{y'}$

(14) Next, equated secret imageis shared using the Diffie- Hellman authentication protocol.

Now, we describe about the secure confidential key management based on diffie-hellman authentication protocol, used in the privilege based advanced haftoning model. An elliptic curve of (x_1, y_1) and (x_2, y_2) points on the curve of elliptic field $GF(2^k)$ which can accessible for any third party authentication. If sender S_i selects a secret value be SK_i $(0 \le SK_{i_x} \le 2^k - 1)$ and it equates $g^x = h(X \oplus SCK_i)$ and forwards with session key SK_i to the receiver R_j. Likewise, on the another hand receiver R_j selects the secret value SK_j $(0 \le SK_{i_y} \le 2^k - 1)$ and equates $g^y = h(Y \oplus SCK_j)$ and forwards with the SK_j to the sender S_i. Then, sender S_i and receiver R_j equates with the public values $g^{x'}$ and $g^{y'}$ in which both the values are matches and therefore it send the secret confidential key for sharing the secret images from sender to receiver in the privilegemodel to provide secure encryption.

In the proposed mechanism uses privilege based advanced haftoning model, it requires two essential keys g^x and g^y are produced from two different parties sender S_i and receiver R_j. The cover image is classified into non-overlapping image segments or block size of 32x32. The process of embedding algorithm in the privilege based advanced halftoning process with error diffusion technique and diffie authentication protocol are explained below.

- Consider a value *p=1024* (As block size of pixels is 1024).
- Identify the 32 positions of secret images and shares embedding in blocks

- Calculate $g^{x'} = \text{mod}\, AK_i$, $g^{y'} = \text{mod}\ AK_j$.
- When it is higher than 32 size, decrease 32 from then value
- Then, obtained value is equated by considering *mod(p-1,* S_i *).*
- Hence, the value of S_i with pixel positions are equated.
- Similarly, identify the value of $g^{y'}$ utilizing R_j
- Combine the embedded bits in the (S_i , R_j) position of the block.

The blocks is plied in the each secret images shares in order to improve the medical images security, once after the adaptive secure confidential key of diffie-hell man authentication protocol in the privilege based advanced halftoning process with error diffusion technique is completed. It is based on the stimulation performances that proposed system proves to obtain the, Peak Signal to Noise Ratio (PSNR), correlation, error diffusion and Similarity Index.

IV PERFORMANCE ANALYSIS

The proposed mechanisms is analyzed in the Matlab 2010b. The experimental results are carried to prove the highest significance level of the proposed method in terms of the accuracy, peak signal-to-noise ratio (PSNR), error diffusion, encryption execution time, and security. The performance analyzes of the obtained results are clearly demonstrated in this section. The proposed method for the privilege based advance haftoning secret sharing scheme with error diffusion technique along with adaptive secure confidential key based diffiehellman based authentication protocol. It reveal about the shares are created based on the privilege of the images pixels for making then secret image sharing scheme that can embed upto 90 kb with pixel size of 1024* 1024color image. The effectiveness of the proposed system based on the PSNR ration of the secret medical image along with stenography images which higher than a10 dB. The proposed model are clearly demonstrated from the Fig.4 to Fig. 13, it evaluates about the process in the each phase in the model, in which step by step process are represented in the experimental results. Therefore, implementation results of the proposed scheme characteristics in the Steganography images of cover images and secret images with PSNR ratio, MSE, NC, SSI are estimated in the table 1. Here, we described about the performance metrics considered in the model are given below

4.1 EXPERIMENTAL RESULTS

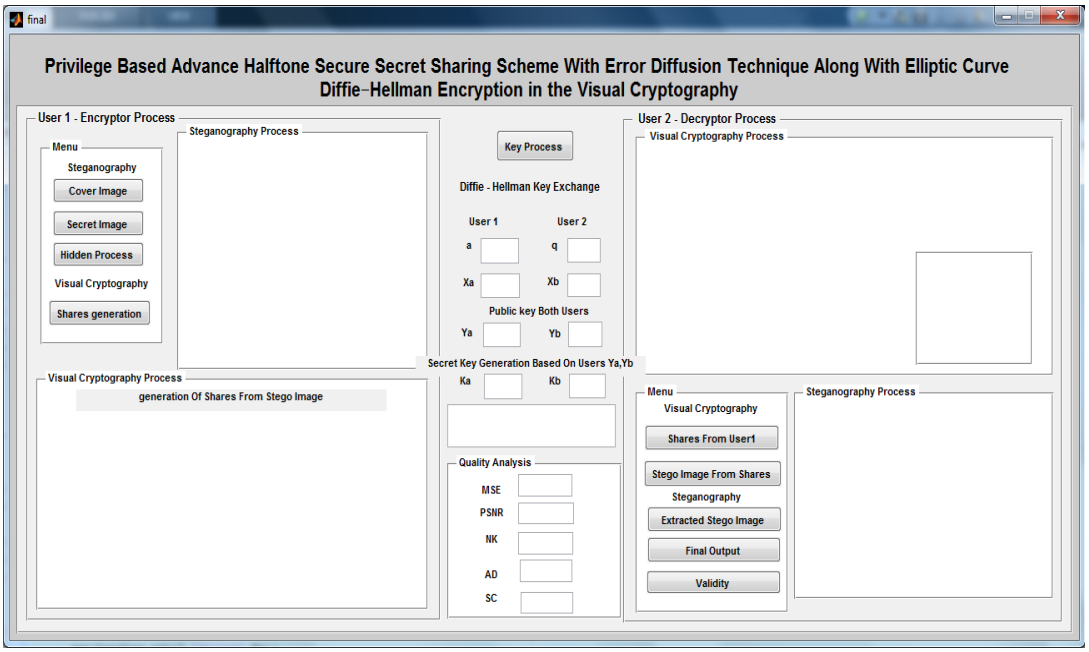

Fig .4 Overview Proposed System

In the Fig 4, describes about the overview of the proposed system in a single GUI in order to make the clear view of the process involved in the model

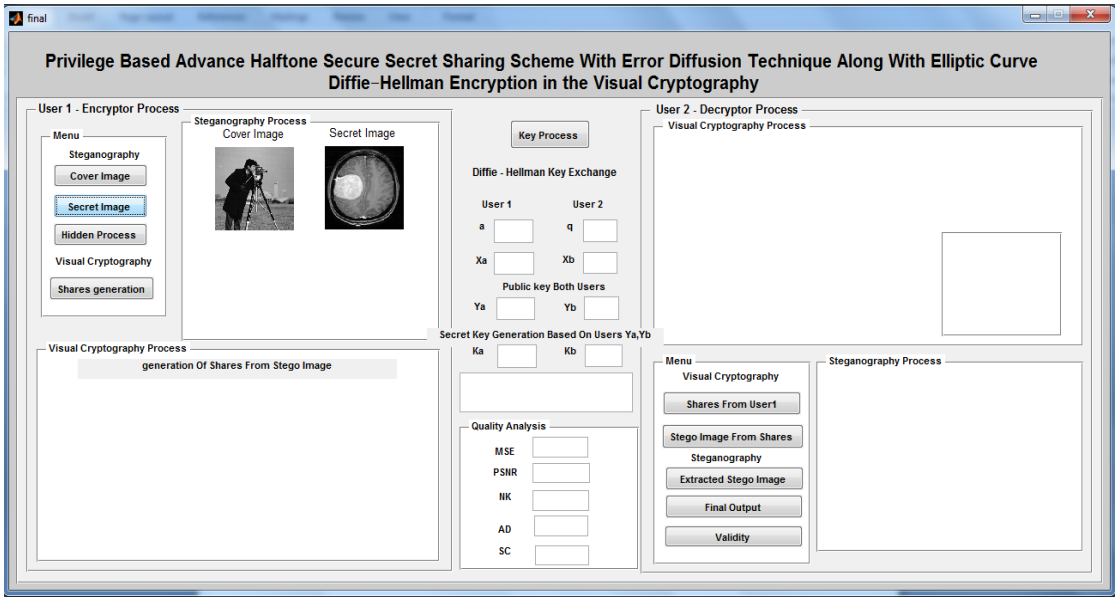

Fig.5 Steganography images of cover images and secret images

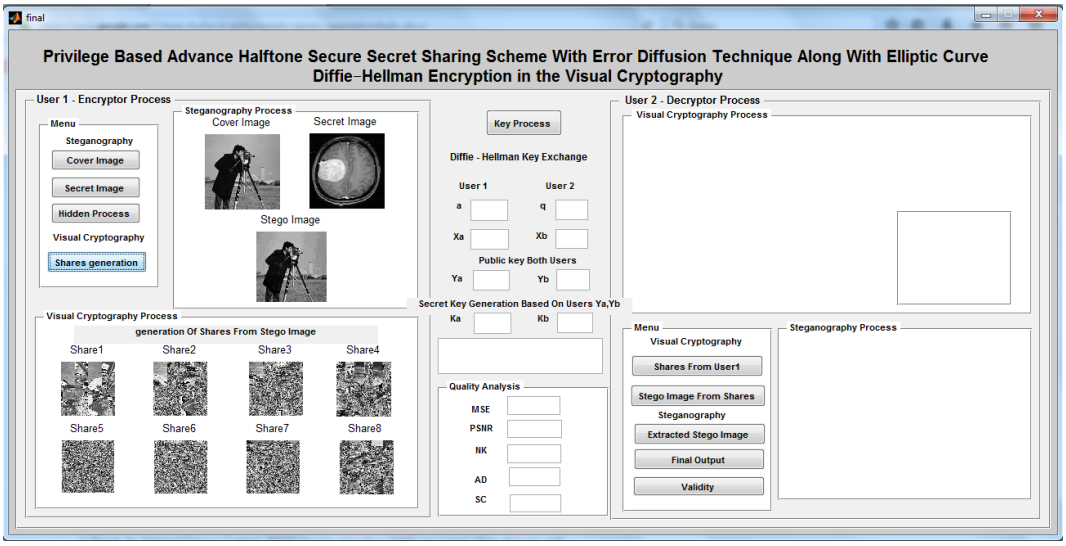

Fig .6 Share Creation

Here, it creates the privilege based shares for the secret medical images in the visual cryptography

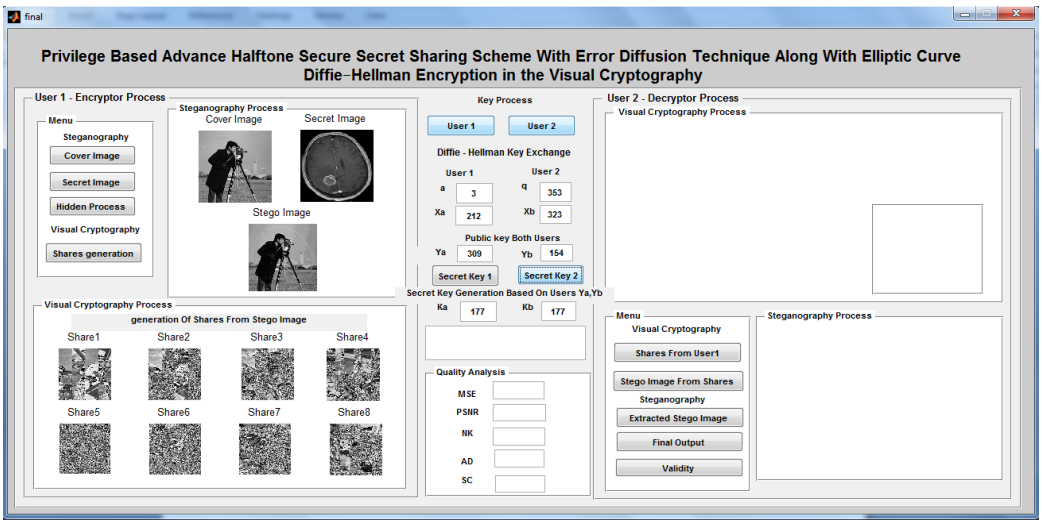

Fig .7 Adaptive secure confidential key Diffie-Hellman authentication protocol

Now, once after the privilege based shares are created in order to provide the security for the secret images, it uses diffie-hellman key authentication protocol in the steganography process in the VC

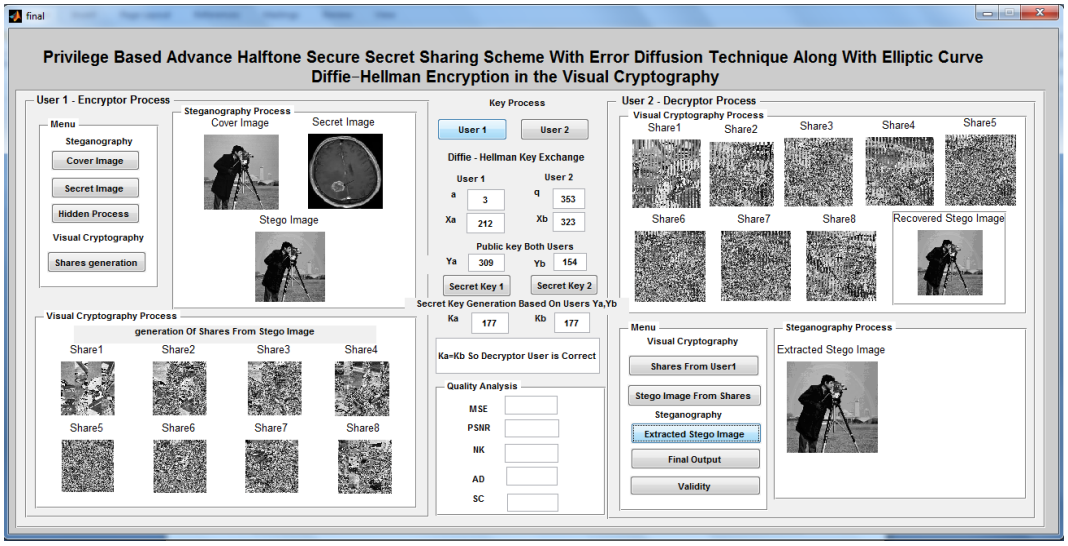

Fig .8 Reconstructed images

In this process, once after the Key verification process, if the key is matched and then by using advance halftoning process it can reconstruct the cover images from the privilege shares.

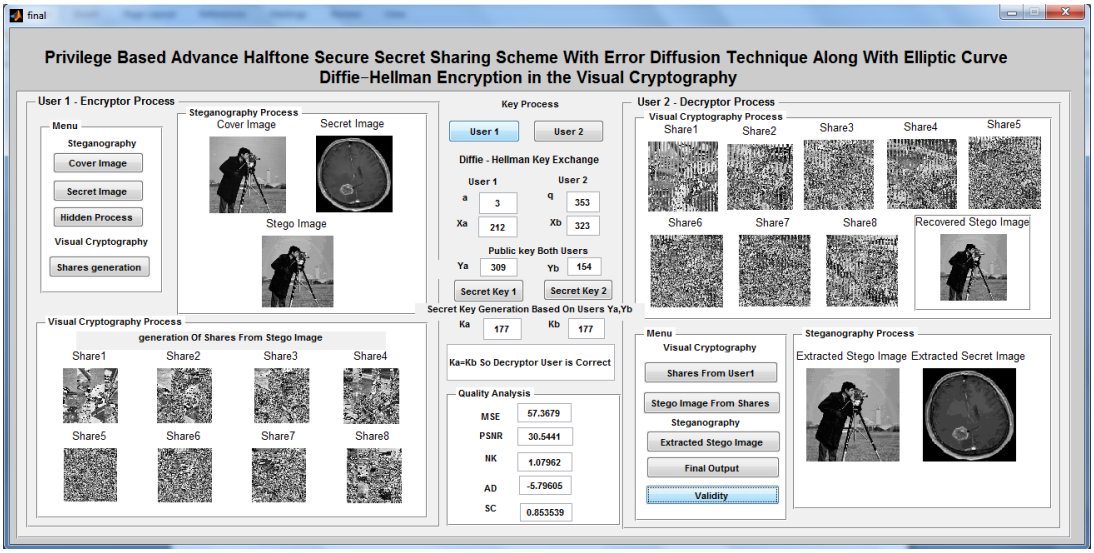

Fig .9 Extracted of the secret images

Finally in the Fig 9, it has obtained the extracted secret images after verification process of the cover images and using adaptive secure confidential key based diffiehellman authentication protocol. In this section , we provide the description of the performances metrics used to prove the effectiveness of the proposed system.

Thus the shares images are containing the secret medical images which is classified into eight shares along with privilege value, it is demonstrated in the Fig .4 . These shares are very significant shares which is transmitted to respondents. Next, elliptic curve diffie-hellman key exchange algorithm is used in the Bit-Plane Complexity Steganography process in the visual cryptography. Once after the key is matched in the verification process and then only the reconstruction or retrieving process for the images has been performed. We reconstruct the Steganography images of the cover image as the confirmation image in the Fig .6. Then retrieve the secret image without any much loss in the Peak Signal to Noise Ratio (PSNR) which is demonstrated in the table 1.

4.2 Peak Signal-to-Noise Ratio (PSNR):

It is equated to analyze the concealing effect in the secret images in the steganography process. It estimates as the ratio between the highest capacity of removing the unwanted noise in the original images and the extracting images in the visual cryptography. It is used to obtain the exactness of the images and its formula is given below and its graph is demonstrated in Fig.11

$$PSNR = 10\log_{10}\frac{M^2}{\frac{1}{m\times n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j)-K(i,j)]^2} \tag{10}$$

Where, M is represented the highest power capacity of the signal, $I(i,j)$ is the original images and $K(i,j)$ is the extracted images in the Steganography process. The highest value of PSNR value proves to efficient than existing methods.

4.3 Normalized Correlation (NC):

The proposed model robustness is accomplished by utilizing the Normalized Cross Correlation (NC) method. It is an effective performance metric to analyze the degree of resemblance (or dissimilarity) between the original and extracted images. The original image and the extracted images are equated and its estimated Normalized Cross Correlation is given below: The equation to compute NC is given in (4) its graph is demonstrated in Fig.12

$$NC = \frac{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} W(i,j)W^{'}(i,j)}{\sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}[W(i,j)]^2}\sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}[W^{'}(i,j)]^2}} \tag{11}$$

Where, *W(i, j)* is represented as original image and $W^{'}(i,j)$ is the extracted secret image. The Normalized Cross Correlation value between 0 and 1. Since the increase in the value can make system more robust.

4.4 MEAN SQUARE ERROR (MSE)

It estimates the average or mean of the square of the deviations or errors in the images is obtained by MSE. It analyze the difference between the original image and the extracted the secret images, which is used to obtain the accurate value in the images and its graph is demonstrated in Fig.13

$$MSE = \frac{1}{m \times n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \tag{12}$$

4.5 STRUCTURAL SIMILARITY INDEX (SSI):

Structural Similarity Index is utilized to identify the resemblance between the original image and extracted secret images, it is designed to calculate the image quality. It is formula represented below and its graph is demonstrated in Fig.14

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{13}$$

Where μ_x , μ_y will be the average of x, y, σ_x^2 σ_y^2 is represented of variance of x and y; hence c1 and c2 is denoted as $c_1 = (k_1 L)^2$, $c_2 = (k_2 L)^2$ are two static variables with dynamic image pixel values.

TABLE 1 : PERFORMANCE METRICS

Metrics	Image 1	Image 2	Image 3	Image 4	Image 5
MSE	60.6593	63.1908	77.0324	57.3679	45.6727
PSRN	30.3018,	30.1243	29.2641	30.5441	31.5342
NC	1.05377	1.05327	1.05516	1.07962	1.07969
SSIM	0.89768	0.90014	0.89366	0.85353	0.85329

TABLE 2: ERROR TABLE

Methods utilized	**Error produced**
Error diffusion	4.89×10^{10}
Advanced Halftoning	2.27×10^{10}
Privilege based advance haftoning	1.89×10^{10}

4.6 **EXECUTION TIME**

Here, in this model we consider the execution time for the encryption of the images under each different bocks size and the average calculation time is represented in table 3 and Fig. 10.

TABLE 3: EXECUTION TIME

Encryption time	**Block Size**
11.96 s	256*256
15.34 s	512 *512
21.31 s	1024 *1024

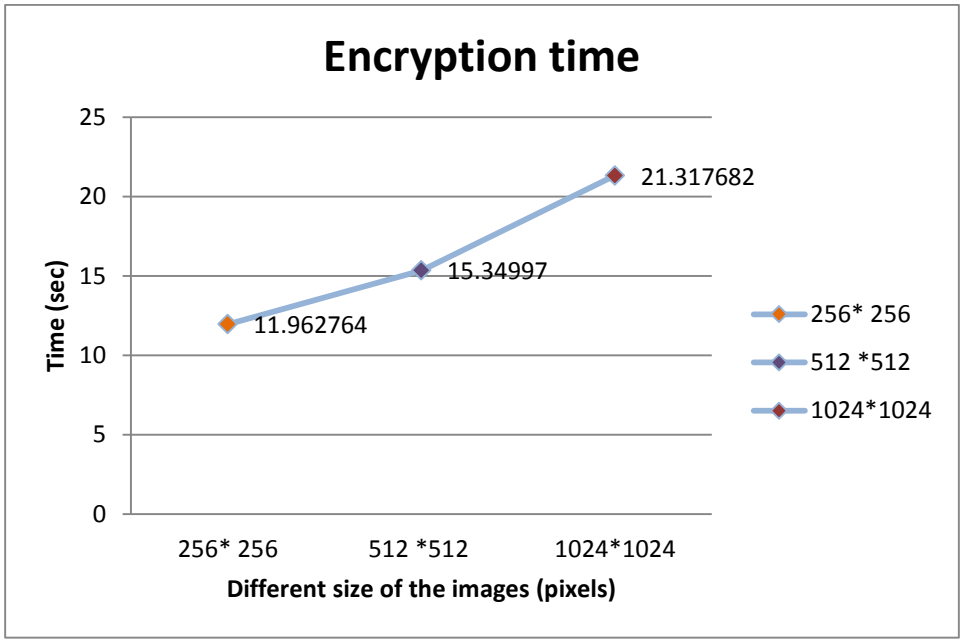

Fig .10 Encryption time

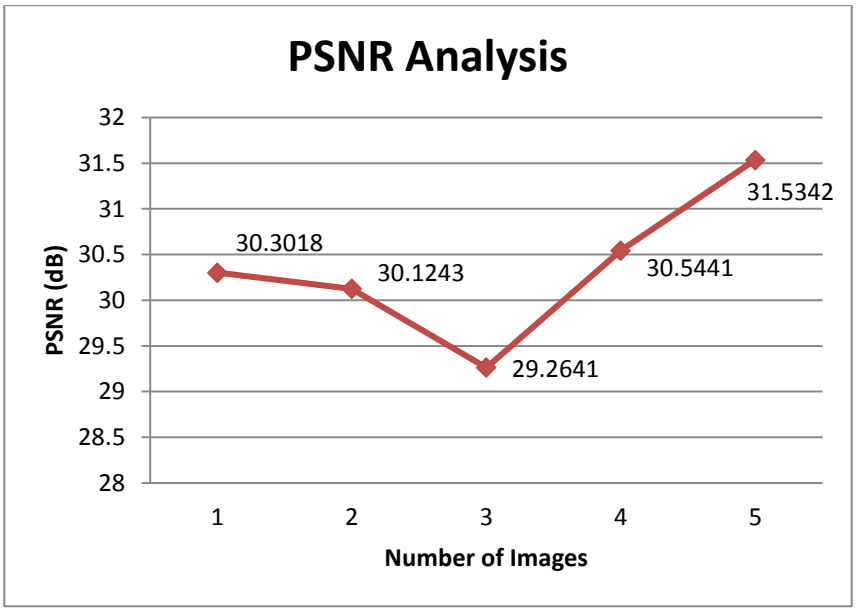

Fig.11 Peak Signal to Noise Ratio

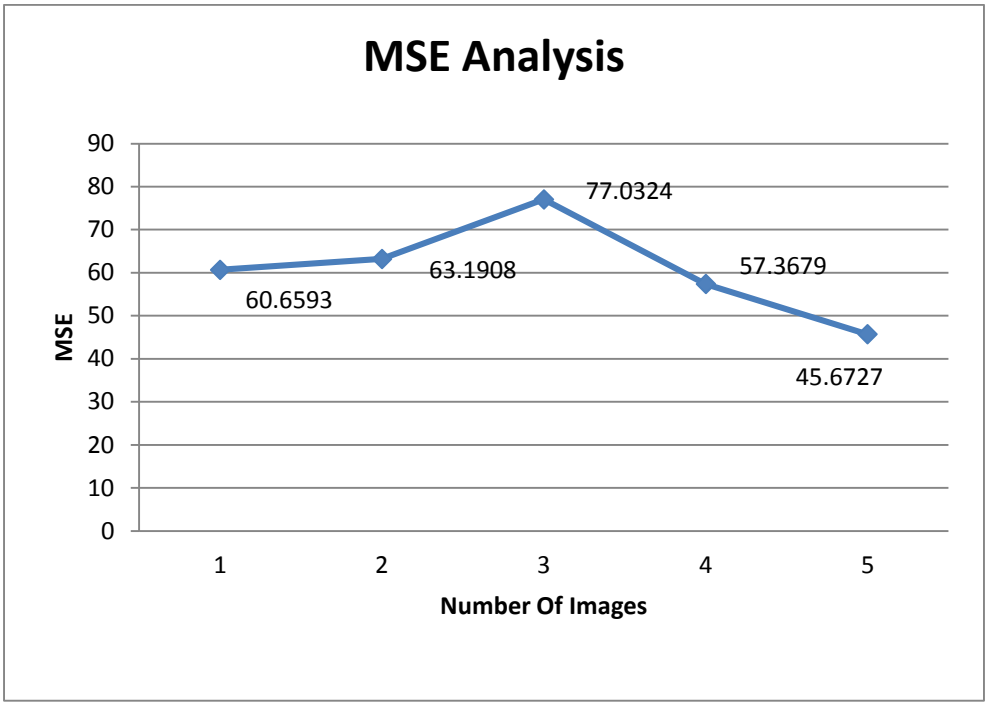

Fig .12 Mean Square Error

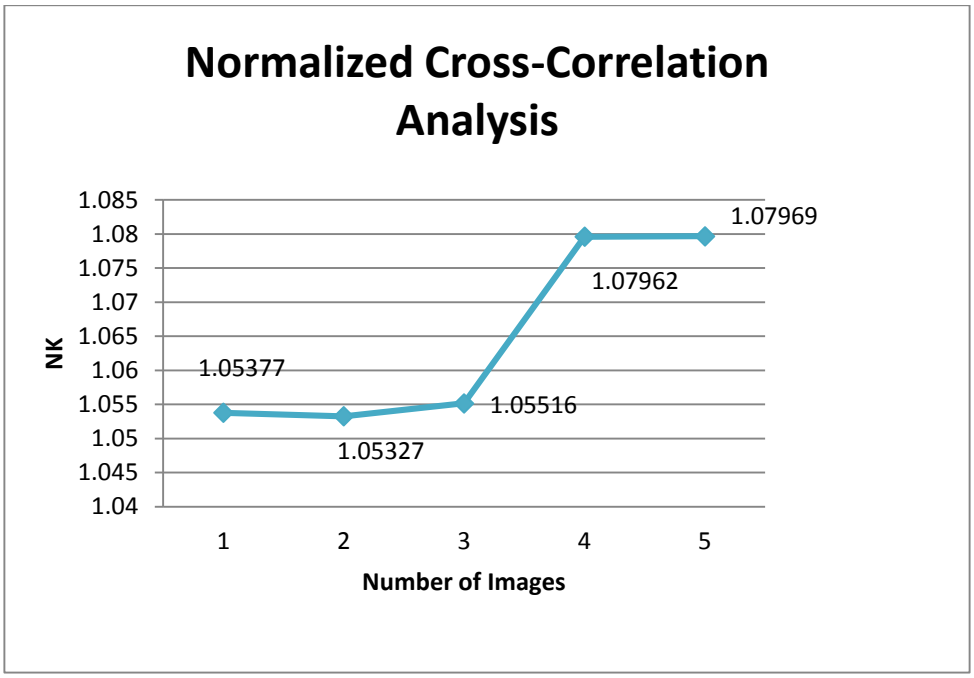

Fig .13 Normalized Cross Correlation Analysis

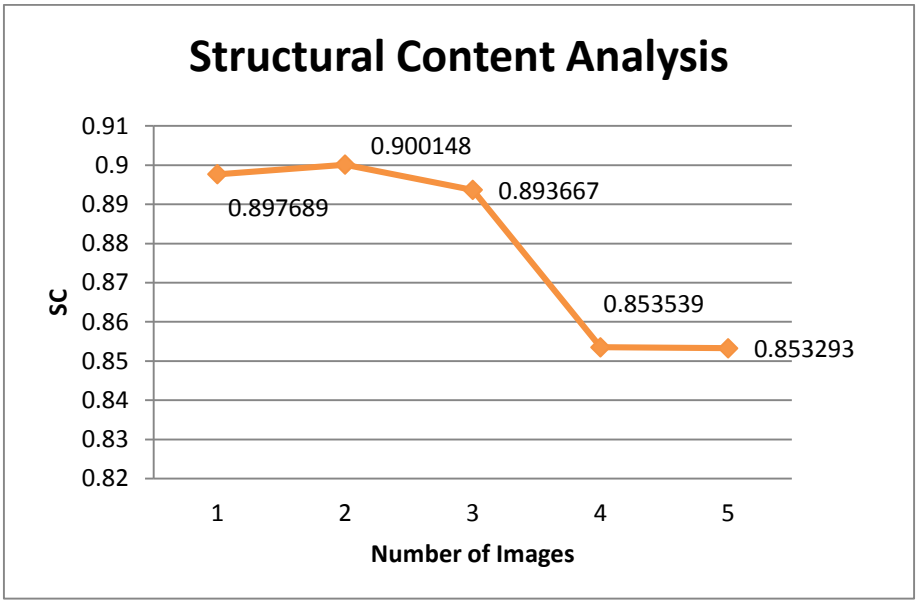

Fig.14 Structure Similarity Index

In our proposed model, we utilized peak signal-to-noise ratio (PSNR) to obtain the image quality of the extraction of the secret image from the original secret images. The peak signal-to-noise ratio analyzes the quality of images by determining the mean squared error (MSE). Later on distinguishing the highest data range and along with its type, for utilizing mean squared error as represented in the Fig.12. Actually, peak signal-to-noise ratio are required to be present with the range of 30dB to 40dB , when the proposed model accomplishes the value in this range and hence it is referred as better visual quality image. When peak signal-to-noise ratio value equals to ∞ that describes about proposed model, it has provided the highest visual quality in the images. To analyze the proposed model accuracy, recovered secret medical image is equated with original image, it is described in the table 1.

The secret image quality is rebuild very effectively by utilizing the error diffusion matrix along with advance haftoning algorithm, error rate of the secret medical image is obtained in the table 2. Therefore, the implemental results would prove that the privilege based advance haftoning secret sharing scheme with error diffusion technique along with adaptive secure confidential key has obtained in table 3, It obtains fastest encryption time with very lower error loss in the proposed model in each channel for the visual cryptography . Thus the privilege model has the fastest encryption time with lower error and achieves secure image or data sharing without affecting the quality of the image.

V. CONCLUSION

In this paper, we propose Privilege Based Advance Halftone Secure Secret Sharing Scheme including Error Diffusion Technique along with Adaptive Secure Confidential Key Based Diffie Hellman Based Authentication Protocol. We make the significant shares which contains the secret data or images in the shares by providing privilege values to the specific participants. Consequently, when a share contains of larger number of black spots in the shares can disclose the secret image at very faster rate, so we provide top privilege to that particular share. Hence, privilege in the share are estimated in order to receive the secret images with privilege level in the advanced halftone secret sharing model along with the error diffusion techniques in order to avoid the noise in the secret medical images. This secret medical image would be used for building the significant and secure transmission of the data or images with the help of adaptive secure confidential key from diffie-hellman authentication protocol which is applied in our model to provide higher image as well as data security. Thus the experimental results of accuracy, Peak Signal-To-Noise Ratio (PSNR), Mean Square Error (MSE) , Normalized Cross Correlation (NC), Structural Similarity Index (SSI), error diffusion, and encryption execution time has proved that our proposed method is very significant than previous methods.

REFERENCES

[1] G. R. Blakley et al . (1979). Safeguarding cryptographic keys, in: Proc. of the National Computer Conf., New York,pp. 313–317.

[2] C.C. Thien, J.C. Lin. (2002). Secret image sharing, Comput.Graph.26 (5) (2002) 765– 770.

[3] S.K. Chen, J.C. Lin. (2005). Fault-tolerant and progressive transmission of images, Pattern Recogn. 38 (12) (2005) 2466–2471.

[4] A. Shamir. (1979). How to share a secret, Commun. Assoc. Comput. Mach. 22 (11) 612–613.

[5] M. Naor and A. Shamir. (1994). "Visual cryptography", Proc. Advances in Cryptology (Eurprocrypt'94), pp.1 -12

[6] C.N. Yang, S.M. Huang. (2010). Constructions and properties of k out of n scalable secret image sharing, Opt. Commun. 283 (9) 1750–1762.

[7] Y.-S. Wu, C.-C.Thien, J.-C.Lin. (2004).Sharing and hiding secret images with size constraint, Pattern Recogn. 37 (7) 1377–1385.

[8] C.-C. Thien, J.-C.Lin. (2003). A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function, Pattern Recogn. 36 (12) 2875–2881.

[9] P. Li, C.N. Yang, C.C. Wu, Q. Kong, Y. Ma. (2013). Essential secret image sharing scheme with different importance of shadows, J. Vis. Commun. Image R 24 1106–1114.

[10] G. R. Blakley. (1970). ”Safeguarding Cryptographic Keys,” Proceedings of AFIPS Conference, vol. 48, pp. 313-317.

[11] T. Monoth and A. P. Babu. (2007). ”Recursive Visual Cryptography Using Random Basis Column Pixel Expansion,” in Proceedings of IEEE International Conference on Information Technology, pp. 4143.

[12] H. J. Kim, V. Sachnev, S. J. Choi and S. Xiang. (2007). ”An Innocuous Visual Cryptography Scheme,” in Proceedings of IEEE-8th International Workshop on Image Analysis for Multimedia Interactive Services.

[13] ChetanaHegde, Manu S, P DeepaShenoy, Venugopal K R, L M Patnaik. (2008). ” Secure Authentication using Image Processing and Visual Cryptography for Banking Applications”, Defence Institute of Advanced Technology, Deemed University, Pune, India.

[14] E. R. Verheul and H. C. A. Van Tilborg. (1997). .”Constructions and Propertiesof*k* out of *n* Visual Secret Sharing Schemes”,.*Designs,Codes,Cryptography*, vol. 11, no. 2, pp. 179-196.

[15] W.-G. Tzeng and C.-M.Hu.(2002). “A new approach for visual cryptography”, Designs, Codes and Cryptography 27, pp. 207–227.

[16] Ching-Nung Yang, Chung-Chun Wang and Tse-Shih Chen. (2009). ” Visual Cryptography Schemes with Reversing”, Department of Computer Science and Information Engineering, National Dong Hwa University, No. 1, Section 2, Da Hsueh Road, Hualien, Taiwan.

[17] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson. (1996). Visual cryptography for general access structures, Inf. Computer. 129(2) 86–106.

[18] Z. Zhou, G.R. Arce, G. Di Crescenzo. (2006). Halftone visual cryptography, IEEE Trans. Image Process. 15(8) 2441–2453.

[19] D. Tsai, T. Chen, G. Horng. (2008). On generating meaningful shares in visual secret sharing scheme, J. Imaging Sci. 56(1) 49–55.

[20] J. Weir, W. Yan. (2010). A comprehensive study of visual cryptography, in: Transac-tions on DHMS V, in: LNCS, vol.6010, Springer-Verlag, Berlin, Heidelberg, pp.70–105.

[21] F. Liu, C. Wu. (2011). Embedded extended visual cryptography schemes, IEEE Trans. Inf. Forensics Secur. 6(2) 307–322.

[22] Y.C. Hou, Z.Y. Quan. (2011). Progressive visual cryptography with unexpanded shares, IEEE Trans. Circ. Syst. Video Technol. 21 (11) 1760–1764.

[23] T.H. Chen, K.H. Tsao.(2011). Threshold visual secret sharing by random grids, J. Syst. Softw. 84 (7) 1197–1208.

[24] T.Guo, F.Liu, C. Wu. (2013). out of k extended visual cryptography scheme by random grids, Signal Process, 90–101.

[25] Zhen, G. Zhao, L. Min, X. Jin, Chaos-based image encryption scheme combining DNA coding and entropy, Multimed Tools Applhttp://dx.doi.org/10.1007/s11042-015-2573-x.

[26] W.-M. Pang, Y. Qu, T.-T.Wong, D. Cohen-Or, P.-A.Heng.(2008). Structure-aware halftoning, ACM Trans. Graph.27, 89.

[27] C.N. Yang, Y.Y. Chu. (2011). A general (k,n) scalable secret image sharing scheme with the smooth scalability, Journal of Systems & Software 84, 1726–1733.

[28] LeinHarn et al. (2013). Group authentication.*IEEE Transactions on computers*, vol. 62, no. 9;September.

[29] Sian-Jheng Lin and Wei-Ho Chung. (2012). A probabilistic model of (t, n) visual cryptography scheme with dynamic group.*IEEE Transactions on Information Forensics and Security*, vol. 7, No. 1;February.

[30] IlkerNadiBozkurt, Kamer Kaya and Ali AydınSelcuk. (2012). Threshold cryptography based on blakley's secret sharing. *IEEE Transactions*, vol.4, 84-92.

[31] Tai- Wen Yue and Suchen Chiang. (2012). A neural network approach for visual cryptography.*IEEE*, Vol. 8;March.

[32] SmithaJhajharia. (2013). Public key cryptography using neural networks and genetic algorithms.*IEEE*, Vol. 45;May.

[33] Y. Liu, M. Hu, X. Ma, H. Zhao. (2015). A new robust data hiding method for H.264/AVC without intra-frame distortion drift, Neurocomputing 151 (3) 1076– 1085.

[34] C.W. Lee, W.H. Tsai. (2013). A data hiding method based on information sharing via PNG images for applications of color image authentication and metadata embedding, Signal Process. 93 (7) 2010–2025.

[35] I Xiang Wang, Qingqi Pei and HuiLi.A. (2014). lossless tagged visual cryptography scheme.*IEEE Signal Processing Letters*, Vol. 22, No. 7;July.

[36] Y.H. Huang, C.C. Chang, C.Y. Yu. (2014). A DNA-based data hiding technique with low modification rates, Multimed. Tools Appl. 70 (3) 1439–1451.

[37] H. Liu, D. Lin, A. Kadir. (2013). A novel data hiding method based on deoxyribonucleic acid coding, Comput. Electr. Eng. 39 (4) 1164–1173.

[38] Q. Zhang, L. Guo, X. Wei,. (2013). A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system, Optik 124 3596– 3600.

[39] C.C. Chang, T.C. Lu, Y.F. Chang, C.T. Lee. (2007). Reversible data hiding schemes for deoxyribonucleic acid (DNA) medium, Int. J. Innov.Comput. Inform. Control 3 (5) .

[40] S.C. Wei, Y.C. Hou, Y.C. Lu. (2015). A technique for sharing a digital image, Comput. Stand. Inter. 40 53–61.

[41] L. Liu, Q. Zhang, X. Wei. (2012). A RGB image encryption algorithm based on DNA encoding and chaos map, Comput.Electr. Eng. 38 1240–1248.

[42] Shu-Fen Tu, Ching-Sheng Hsu. (2015). Digital Watermarking Method Based on Image Size Invariant Visual Cryptographic Scheme, Proceedings of the 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing, pp 362-366, IEEE Computer Society Washington, DC, USA.

[43] Vankamamidi, Naresh and Nistala. (2015).A new two-round dynamic authenticated contributory group key agreement protocol using elliptic curve Diffie–Hellman with privacy preserving public key infrastructure, Sadhana, Indian Academy of Sciences,Springer link, volume 40, Issue 7, pp 2143-2161.