Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 11, Number 5 (2015), pp. 3763-3775

http://www.ripublication.com

A Secure Image Transmission scheme based on Visual Cryptography for Commercial Platform

Rajesh Kumar N[1] and Raajan N R[2]

[1]Assistant Professor, [2]Senior Assistant Professor,
[1]Department of Computer Science and Engineering, Srinivasa Ramanujan Centre,
[2]Department of Electronics and Communication,
School of Electrical & Electronics Engineering, [1,2] SASTRA University, India-613 401
Corresponding author, e-mail:[1] rk6030@gmail.com

Abstract

Phylogeny of banking (E-Commerce) departed through automated teller systems (ATMs) and incorporates banking through mobile systems, bill payment gateways, Online and fund transferring schemes. These online transactions are performed using the password, secret key and OTP (one time password). However it is insecure whereas sending the password file to the customer through the internet. In this nominated work we enforced an image protection mechanism for banking process to protect the password file using the visual cryptography for binary images. The term visual cryptography is a new mechanism, which dealt with information security and proceeds with simple mechanisms and not with huge computationally intensive technique of traditional crypto schemes. Visual cryptography allows only the visual content, which is in the form of pictures; text and written materials are enciphered in such a manner and deciphering scheme is executed by the human visual system, without any background of the complicate crypto schemes. This anticipated work nominates a new glide path of 2 out of 2 (4 pels) secret sharing scheme horizontally to protect the images in binary form. The outcomes of the anticipated research work depicts that the projected mechanism has perfectly applicable and achieves for binary images.

Keywords: Code table, Diwy, Pel elaboration, Secret sharing, Visual secret sharing

I. Introduction

Security over the Information plays a lead role in network communication. The

terminus Cryptography goes along with the chore of composing an enigma code that is only experienced to the aimed user community confiding the third parties with no lead about the substance. Cryptographic mechanisms capers a lead persona to defend the sensible data from unauthorized usage. Whereas proceeding with communication between diligences, there are some specific protection speculations such as integrity, non-repudiation, authentication, and privacy/confidentiality. To meet the above suppositions, various crypto techniques are being used. Thus protection is attained by employing effective algorithms of crypto schemes. In cryptography; the user's information is protected by transforming it into the unreadable format. Figure 1 illustrates two phases i.e. encryption and decryption in the process of communication using cryptography.

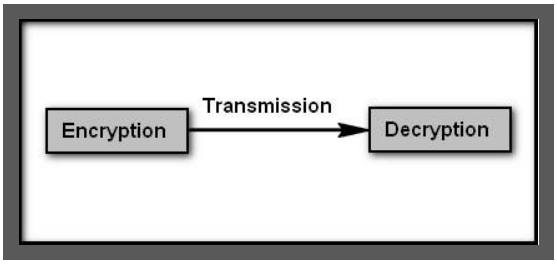

Figure 1. Phases in cryptographic communication

The procedure encryption performs summon of transforming the secret info into something that appears to be random and meaningless. Decryption is the process of converting Ciphertext back to plaintext. Image encryption has been implemented in various fields such as cyberspace communications of military and non military organizations, processing medical images and animations.

Internet plays a lead role in the world of electronic communications, which is the backbone to forward information among various sources. In the running era of the e-commerce, a contiguous need of problem solving ensures safety over the content is increasingly high in the open network environment. To ensure content confidentiality in various fields such as banking, tenders etc., various enciphering schemes are followed. With the help of such existing schemes the confidential contents such as online banking password, secret key and OTP (one time password) can be easily identified by intruders.

1. Visual Cryptography

The technique visual cryptography [14] (VC) was primitively fabricated and originated at the Eurocrypt conference in the year 1994 by the researchers Shamir and Naor. It is a pack of crypto techniques that allows the deciphering of hidden pictures without any crypto schemes and the term VC is pertained to human visual system [1, 13, 21]. It is a raw scheme that follows the theme of veiling mysteries within the images. The primary representation of VC actualizes a cryptographic technique named as secret sharing scheme (SS) [10, 11]. In the context of visual secret sharing

(VSS) scheme [4, 5], a secret image is busted up into 'K' number of shares and the person with all the 'K' shares can only decrypt the image, if any one the share is missing then it is impossible to get the original image with 'K-1' shares [8]. All the created shares are printed on a detach lucidity, and decryption procedure can be done by shares overlaying [4]. To get back the original image all the 'K' number of shares needs to be overlaid properly.

2. Pixel Expansion

Pixel expansion is a proficient technique of visual cryptography, which could be used to protect [16] the digital images. Generally the pixels of the image are sub divided into 'K' number of smaller blocks and the blocks are always the equivalent number of blocks with white (transparent) and black values. If a pixel or simply pel is alienated into two parts [12], then the resultant value is one white pel (W) and one black pel (B) and if the pel is alienated into four equal blocks, then the resultant block holds two white and two black pels. If the pels of 'block I' has a given state, the pel of 'block II' has any one of two states, that is either identical or inverse of 'block I'. If the pels of 'block II' is alike to 'block I', then the overlaid pel will be both half-black pel and half-white pel. This overlaid pels are said to be as gray or empty pels. If the pels of the 'layer-1' and 'layer-2' are upturned or conflicting, then the covered description will be fully black and the pel is called as 'Information Pixel'.

The persisting part of the article is machinated as follows. The Section II gives a summarizing review of some recent works of the 'Visual Cryptographic' technique for protecting digital images. The anticipated forceful protection proposal is offered in the Section III. In Section IV we experimentally evaluate these diwy sharing scheme for various commercial applications. Finally, the conclusions are given in Section V.

II Literature Survey

1. Traditional Visual Cryptography:

A secret share or secret is something which is kept from the knowledge of any but the initiated or privileged. Secret sharing dealt with a method by which a secret share [3] can be distributed between participants' group, whereby each applicant of the group is apportioned a piece of the secret share and it is simply denoted as '*share'*. The original content can only be restored only, when adequate numbers of shares are coalesced. The information about the secret cannot be obtained if the shares are separated. That is, the shares are completely useless whereas they are separated. In the scheme of secret sharing, the secret [7] is divided into a number of shares and distributed among n persons. When any k or more of these persons (where $k \leq n$) bring their shares together, the secret can be recovered. However, if k-1 persons attempt to reconstruct the secret, they will fail. Due to this threshold scheme, we typically referring the sharing (secret) system as a (V, K)-threshold scheme or *V-out-of-K* secret sharing [15].

The human eyes can perform the decryption only if the V shares are stacked together. The above will permits anyone to access the system without the background of crypto schemes and its associated computations. This is major benefit of the mechanism

visual [6] cryptography (VC) as compared with the other popular and conditionally secured crypto techniques. The method VC is highly secured and it can be implemented easily in both the hardware and software devices. A secret image is to be diwied instantly through the electronic medium; alternatively the secrets can be published out into foils and layered, disclosing the secret.

The sharing scheme of the secret is based on the Lagrange interpolation which is given by Shamir, in which a set of points is given. i.e., (x_i, y_i), where i = 0, 1, 2, 3,...,k-1, the Lagrange interpolation polynomial can be constructed through the formula which is stated in the equation 1.

$$p(x) = \sum_{i=0}^{k-1} y_i \prod_{i \neq j} \frac{x - x_i}{x_j - x_i} \quad \textbf{(1)}$$

Given a secret, it can be easily shared using this interpolation scheme. If $GF(q)$ denotes a Galois field ($q > n$), the following polynomial is constructed by choosing proper coefficients $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}$ from $GF(q)$, which satisfy the equation given in equation 2.

$$f(x) = s^* + \sum_{i=0}^{k-1} \alpha_i x^i \quad \textbf{(2)}$$

Where s^* is the secret key. The coefficients are randomly chosen over the integers [0, q) and the details are provided in. Suppose $s_i = f(\alpha_i)$, i = 0, 1, 2. . . n, each s_i is known as a share and they can all be delivered to different persons. Now we would like to reconstruct the original secret. Suppose k people have provided their shares s_i, i = 1, 2. . . k Finally Lagrange interpolation polynomial is utilized to reconstruct the original secret. The pattern is stated in the equation 3.

$$p(x) = \sum_{i=0}^{k} s_i \prod_{i \neq j} \frac{\alpha - \alpha_i}{\alpha_j - \alpha_i} \quad \textbf{(3)}$$

Where addition, subtraction, multiplication and division are dened over $GF(q)$:
$P(\alpha_i) = s_i$, i= 1, 2, . . . , k, $s^* = P(0)$. Thus we can attain the novel secret s^*.

2. V-out-of-K secret sharing Scheme

Imparted the input message or image, 'N' numbers of foils are generated. So that the input image (secret message) is seeable if any *'K'* of them is piled together. The original image or message remains concealed if some of the 'S' foils are piled together where $S < K$ [9]. Each pel appears within the 'N' variants s (upgraded) or shares per transparency. The shares hold an assortment of 'M' black-subpixels-and-white subpixels and are formatted together intimately and the arrangement can be stated as a Boolean matrix *P, where P='n' × 'm'* and the construction can be described as:

$P = (P_{ij})_{m \times n}$ where P_{ij} = 1 or 0 *i.f.f.* the j^{th} sub-pel of the ith share is either black or white in color.

Significant parameters of the strategy are:

- '*m'* is the total number of pels in share. This narrates the resolution loss as compared with the original and recovered image.
- '*α'* is the relative weight difference between the mixed shares that comes from a black and white pels of the original image. i.e. the contrast loss in image.
- γ is the size of the group of X_0 and X_1. X_0 refers to the sub-pel shares model for a white pel and X_1 refers to the shares sub-pel patterns for a black pel.

The Hamming weight H(V) of the ORed m-vector V is rendered by the visual system as follows:
A white pel is rendered if $H(V) < d\text{-}\alpha$ and black if $H(V) \leq d$, m for some fixed threshold $1 \leq d \leq m$ and a relative difference where $\alpha > 0$. The generation of shares can be demonstrated clearly by using a 2 out of 2 VSS scheme (universally defined as (2, 2)-VCS). The coming section defines the collections of 2 × 2 matrices:

$$M_0 = \left\{ \text{all matrices prevailed by permuting the columns of } \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \right\}$$

$$M_1 = \left\{ \text{all matrices prevailed by permuting the columns of } \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \right\}$$

Through the pels expansion scheme, one pel from the original image is elaborated into four pels. The shares can be yielded in the following mode:

- If the pel of the original binary image is white, then randomly pick the identical pattern of four pels for both shares.
- If the pel of the original image is black, then pick a complementary pattern pair, i.e., the patterns from the same column which is stated in the Figure 2.

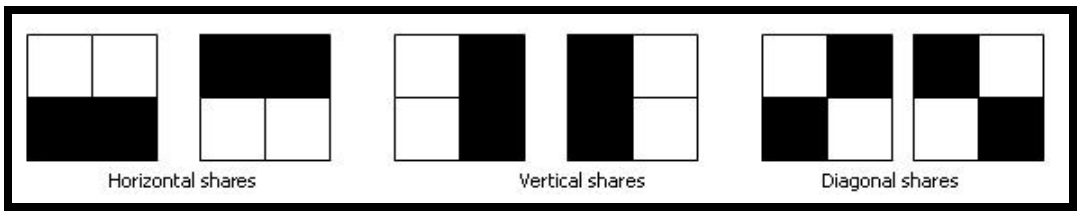

Figure 2. Various modes of the secret shares

When the shares are layered and the shares are ordered properly, the black pels in the conflated shares are comprised by the Boolean-OR of the matrix rows. The pels can be ordered in several modes within the matrix. Visual delegacy of the several types of shares pattern is stated in Fig. 2 and the single shares holds no hint regarding the pel color and also it becomes unimaginable to decipher the shares [20].

3. Recursive Visual Cryptography

A recursive style of secret sharing takes into account a set of two shares [17] which contain more than one secret [2]. Recovering this secret requires rotation or shifting of the share to different locations on the corresponding share.

Let $S2 = S1 \oplus A$, then $A = S1S2$. $S1$ and $S2$ are representations of shares that overlay to generate the secret image and it has the dimensions $m \times n$. Let A be an $m \times n$ matrix such that 1 represents a black pel in the image (secret) whereas 0 represents the white pel of the image.

S1 is created which is of size $m \times n$ of random bits. Half black/half white is represented using 1 and 0 represents the half White / half black pixels [19]. Therefore we have an image which is a matrix of bits. Thus the complete share is generated in random manner. The share two (share-2) is produced by comparing the image and the share one (share-1). The following Figure 3 represents recursive secret sharing process [18].

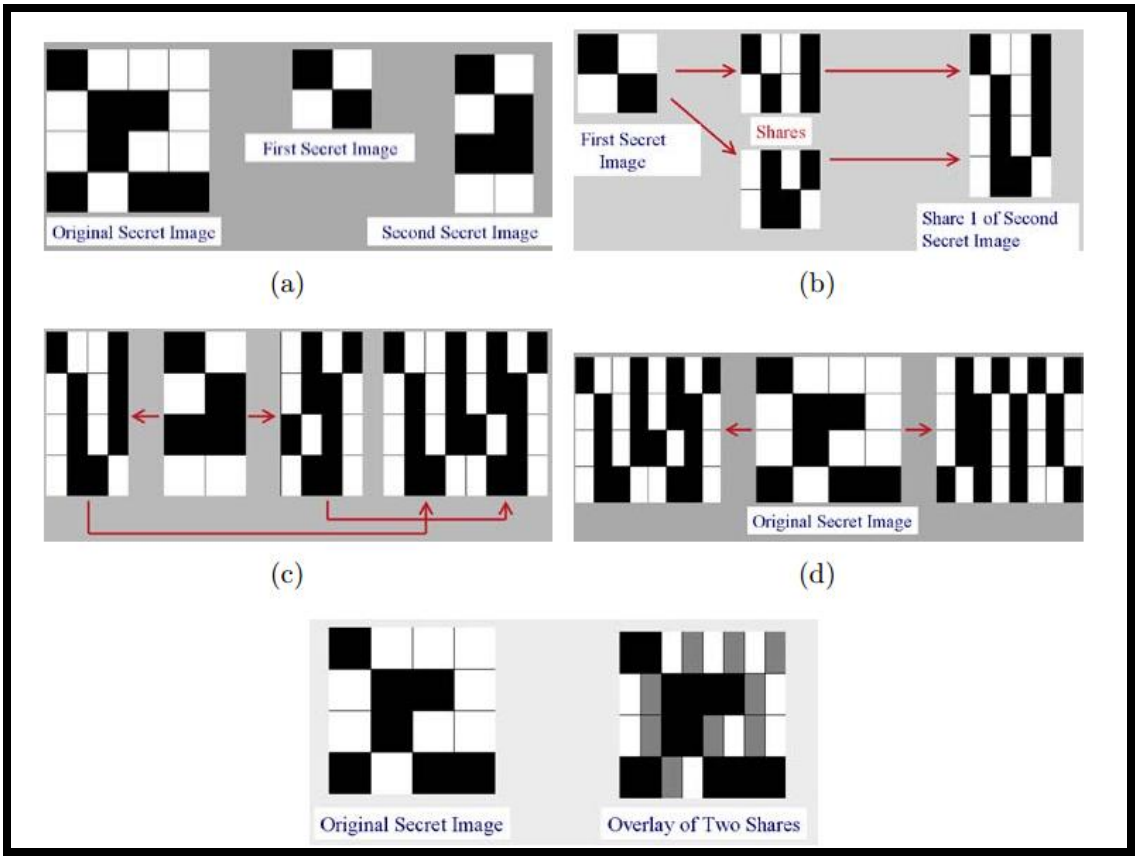

Figure 3. Recursive diwy schemes

III. PROPOSED SCHEME

The proposed (2, 2)-Visual Cryptography Diwy (VCD) sharing mechanism has two methods. The secret image has been encrypted to create a meaningful shares using 2

out 2 VSS (2 pels per pel) and 2 out 2 VSS (4 pels per pel) method. The structure of proposed secret sharing is depicted in Figure 4.

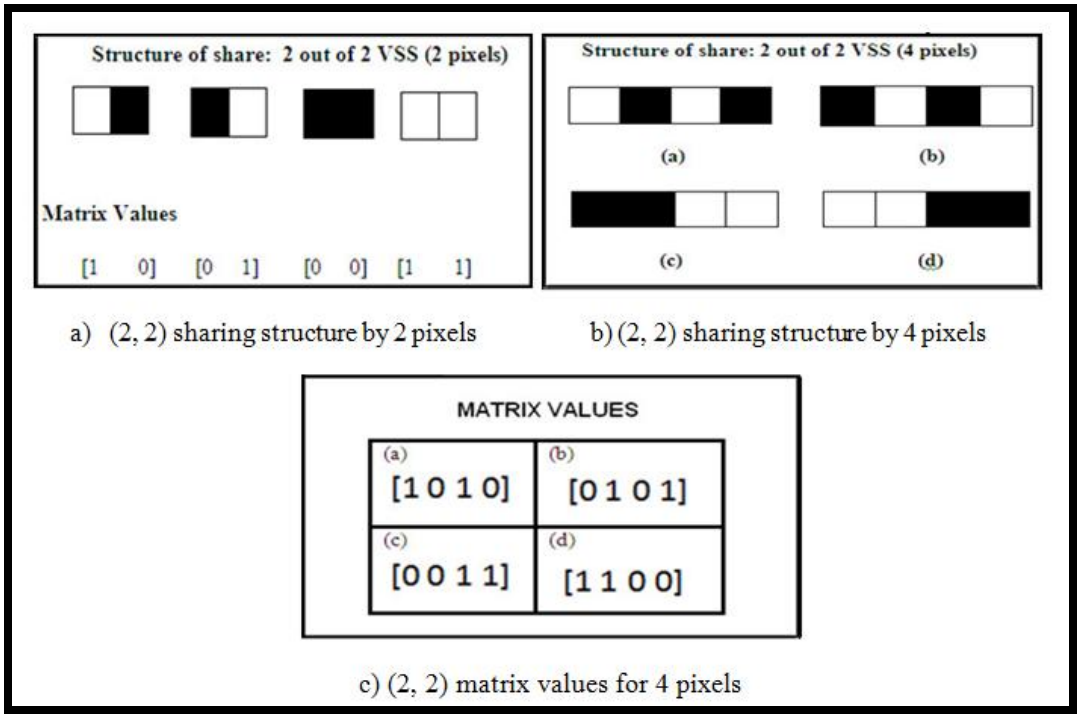

Figure 4. (2, 2) sharing structure and matrix representation

The definition of access code to reveal the secret image is described below:

Definition: Let $\mathcal{P}$ denotes a set of elements, $\therefore \mathcal{P} = \{1, 2, 3\ldots\ldots\ldots, n\}$ .In each element in the set $\mathcal{P}$ are called participants. n-No. of participants involved to recover the secret image in the set. The set $\mathcal{P}$ contains both qualified participants and forbidden participants are called access code. This proposed visual diwy sharing scheme for set $\mathcal{P}$ of 4 participants is a mechanism to encipher a secret image I into 4 stego images.

The symbols are used in the mechanism to define the access code.

$2^{\mathcal{P}}$ set of all subset of participants

Γ_Q Qualified set

Γ_F Forbidden set

$$\therefore \Gamma_Q \in 2^{\mathcal{P}} \quad \textbf{(5)}$$

$$\Gamma_F \in 2^{\mathcal{P}} \quad \textbf{(6)}$$

$$\Gamma_Q \cap \Gamma_F = \emptyset \quad \textbf{(7)}$$

Access code for VCD = (Γ_Q, Γ_F)

Any Γ_Q sets can reconstruct the secret image from the shares.

Any Γ_F set revealed no information.

For example,

The number of participants in the set is 4.

$\therefore$ n = 4,

The participants are denoted in the set P = {1, 2, 3, 4}.

Possible Access structures,

$$A = \{\{1, 2\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}\}$$

Authorized access structure to reconstruct the secret image

$$A_{min} = \{\{1, 2\}, \{3, 4\}\}$$

Unauthorized access structure $\overline{A}$ is specified by the access structures

$$\overline{A} = \{\{1\}, \{2\}, \{3\}, \{4\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}\}$$

1. VCD MECHANISM (Visual Cryptography Diwy)

A binary image is taken as an input image. The number of transparency (shares from the secret) would be needed to hide the secret into meaningful shares are represented by the value two and number of secret shares are desired to reconstruct the image (secret) is represented by two. So this method is called two out of two scheme [(2, 2) VCD scheme]. Figure 5 illustrates the overall layout of the proposed scheme.

The VCD mechanism consists of two stages.

1. Selection procedure for the encryption scheme
2. Pel elaboration process

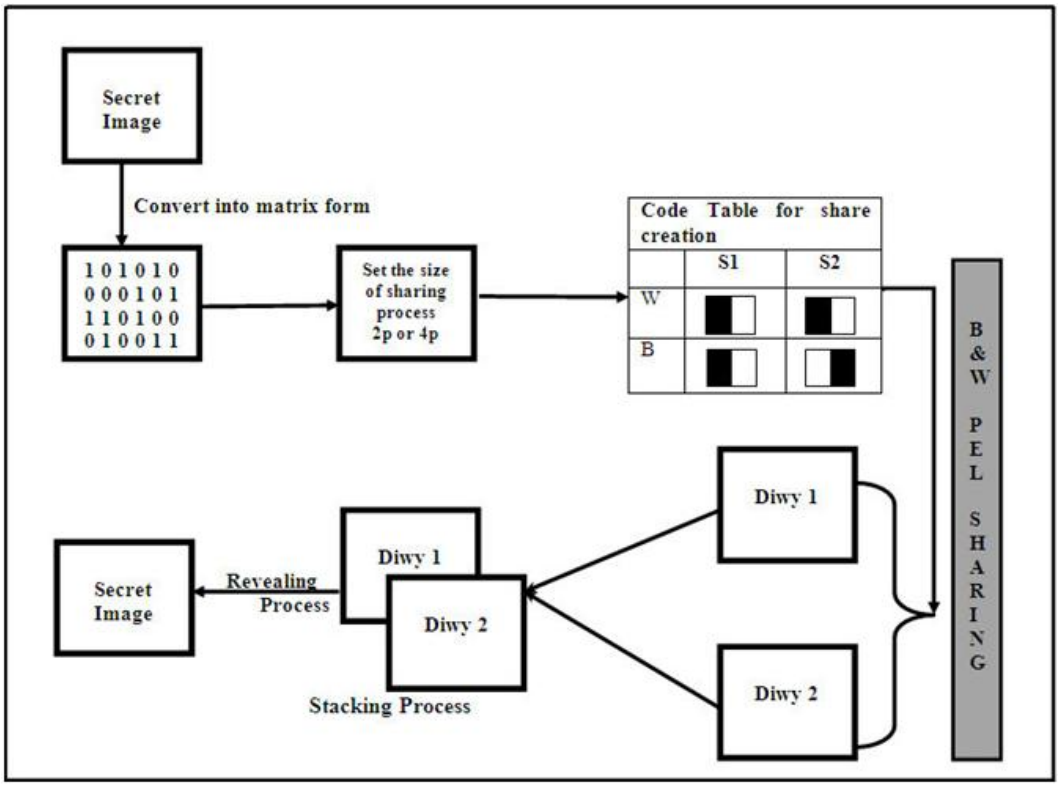

Figure 5. An overview of VCD Mechanism

2. Phase I-Visual Cryptography-Selection procedure for the Encryption Scheme
In this phase we will start the visual cryptography encryption with binary secret image and in this scheme we have implemented 2 out 2 visual secret sharing (VSS) schemes. Initially the secret image is converted into matrix format. The two dimensional matrix contains m × n pixels. It also contains collections of black and white pels. In visual cryptography each pel is handled separately based on the code table to create a share images. This proposed scheme we can create a share images using pel expansion method. Pel expansion is an effective sharing method to disorder the secret image. There are two types of pel expansion methods are included in this proposed work.

- 2 out of 2 VSS (Visual Secret sharing) mechanism (2 sub pels)
- 2 out of 2 VSS (Visual Secret sharing) mechanism (4 sub pels)

After setting the, each pel in the secret image is enciphered into a pair of black-pels-and-white pels in each of the two shares. The sharing process is discussed in Phase II.

3. Phase II-Pel elaboration process
In this phase the encoding scheme performs sharing a binary image into two different transparencies like that diwy1 and diwy2. To share a binary image the proposed idea refers the code table to implement the black & white pel processing. Each pel in the

secret image is divided into a black & white or white & black sub-pel based on the code table procedure. The possible combination for the black & white pel processing is illustrated below:

W-White	**B-Black**
1) WBWB	[1 0 1 0]
2) BWBW	[0 1 0 1]
3) BBWW	[0 0 1 1]
4) WWBB	[1 1 0 0]

Pel '*p*' is taken from image (secret), if the pel '*p*' is white then one of the first two rows are selected from the code table. Else if the pel '*p*' is black one of the last two rows are selected from the code table. The selection is randomized such that each row is selected with a 50% (1/2) probability for 2 sub-pels and 25% (¼). Now the first four sub-pels in that column are allotted to diwy 1 and the following four sub-pels are allotted to create a diwy 2 image. The pixel is divided into four sub-pels based on the code table; each share image contains two white pel and two black pel. Independent of whether p is black secret pixel or white pixel, the pixel p is encoded into four sub-pels stated in above combination with equal probabilities. This is the sharing process to construct the share images from the secret image. The two share images indicate the 2 out of 2 scheme and each share contains the equal probability of black and white pels. So this proposed scheme constructs highly secure shares than traditional visual cryptography and there is no clue to hack the cryptanalyst. The code table is shown in the Table 1.

Table 1. Code Table

Secret Image Pixel	Diwy 1	Diwy 2	Stacked Image
Probability	P=1/4	P=1/4	P=1/4
			
			
			
			

IV. Experimental evaluations

The proposed visual cryptographic scheme achieves effective embedment of the images (Diwy or shares) into the secret image, which is shown in the Figure 6. It also shows the encrypted digital signature shares and it's decoding process. Additionally the proposed visual cryptographic diwy sharing scheme is used to protect the 4-digit ATM secret Pin number and password for Internet banking which is stated Figure 7 and Figure 8.

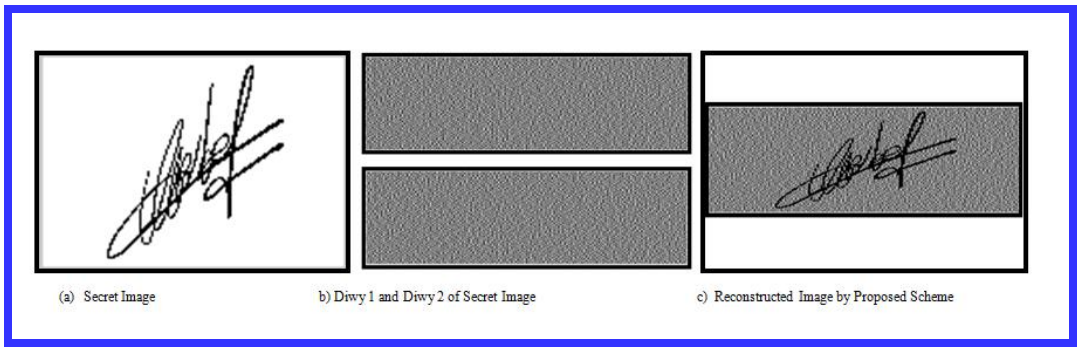

Figure 6. (2,2) VCD scheme staking result for digital signature

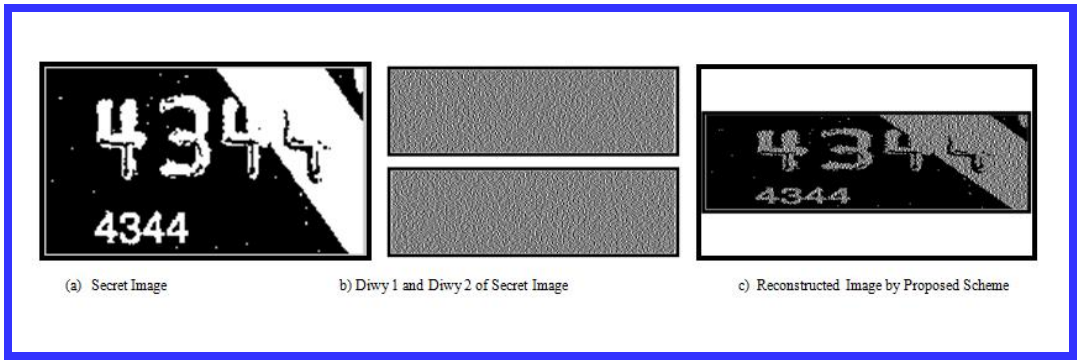

Figure 7. (2,2) VCD scheme staking result for ATM pin

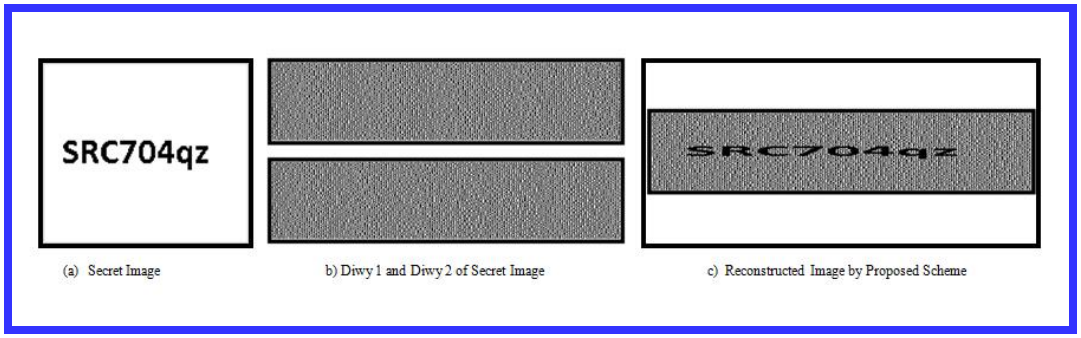

Figure 8. (2,2) VCD scheme staking result for password

5 Conclusions

The term Visual cryptography (VC) is a new innovative practice that has been practiced by various nations for secured data transmission of hand written materials, printed materials, text-images, online voting etc. Lot of research topics about visual secret sharing scheme is widely investigated. But the proposed (2, 2) visual cryptographic diwy (VCD) scheme is more effective than traditional visual cryptography. The two share are aligned properly we can reveal the secret image. Any n-1 share or more some shares grants no clue about the secret content of the image. One of the most important features of this proposed technique is the shares are expanded horizontally and it has increased the security of E-Commerce applications and hence through this approach we can perform secured transmission of the e-banking contents such as Debit/Credit card PIN, One time PIN etc.

REFERENCES

[1] Adi Shamir., 1979,"How to share a secret", Communications of the ACM. 22(11):612-613.

[2] Blundo C, De Santis A, and Naor M., 2000, "Visual cryptography for grey level Images", Inf. Process. Lett., vol. 75, pp. 255-259.

[3] Chang C.C, Hwang R.J., 1998,"Sharing secret images using shadow codebooks", Inform. Sci. 111 335-345 (1998).

[4] Chih-Ching Thien and Ja-Chen Lin., 2002,"Secret image sharing, Computers & Graphics", 26:765-770.

[5] Ching-Nung Yang., 2004 ,"New visual secret sharing schemes using probabilistic method", Pattern Recognition Letters, 25(4):481-494.

[6] Geum-Dal P, Eun-Jun Y, Kee-Young Y., 2008 ,"A New Copyright Protection Scheme with Visual Cryptography", Second International Conference on Future Generation Communication and Networking Symposia, pp. 60-63.

[7] Jagdeep Verma, Dr.Vineeta Khemchandani., 2012,"A Visual Cryptographic Technique to Secure Image Shares", International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622 Vol. 2, Issue1, Jan-Feb, pp.1121-1125.

[8] Jayanta Kumar Pal, Mandal J.K and Kousik Dasgupt., 2010, "A (2, N) Visual Cryptographic Technique For Banking Applications", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October.

[9] MacPherson L. A., 2002,"Grey Level Visual Cryptography for General Access Structures", M.S. thesis, Univ. Waterloo, Waterloo, ON, Canada.

[10] Moni Naor and Benny Pinkas., 1997, "Visual authentication and Identification", In CRYPTO, pages 322-336.

[11] Naor M and Shamir A., 1994, "Visual Cryptography Advances in Cryptology", Eurpocrypt'94, Springer-Verlag, Berlin, pp.1-12.

[12] Rezvan Dastanian and Hadi Shahriar Shahhoseini., 2011,"Multi Secret Sharing Scheme for Encrypting Two Secret Images into Two Shares",

International Conference on Information and Electronics Engineering IPCSIT vol.6 IACSIT Press, Singapore.

[13] Tapasi Bhattacharjee, Jyoti Prakash Singh and Amitava Nag., 2012, "A Novel (2, n) Secret Image Sharing Scheme", Procedia Technology 4 619-623.

[14] Tsai C.S, Chang C.C, and Chen T.S., 2002, "Sharing multiple secrets in digital image", Journal of Systems and Software, Vol. 64, pp. 163-170.

[15] Verheul E and Tilborg H.V., 1997, "Constructions and properties of k out of n visual secret sharing schemes", Designs, Codes and Cryptography, pp.179-196.

[16] Wei-Kuei Chen., 2013, "Image sharing method for gray-level images", The Journal of Systems and Software, 86 581-585.

[17] Wei-Qi Y, Duo J. and M. S. Kankanhalli., 2004, "Visual Cryptography for Print and Scan Applications", International Symposium on Circuits and Systems. pp-572-575.

[18] Yu-Shan Wu, Chih-Ching Thien and Ja-Chen Lin., 2004, "Sharing and hiding secret images with size constraint", Pattern Recognition 37 1377-1385.

[19] Zhi Zhou Arce G.R, Di Crescenzo G., 2006,"Halftone Visual Cryptography", IEEE Transactions on Image Processing, Volume: 15, Issue: 8, pp-2441-2453.

[20] Xuehu Yan · Shen Wang Ahmed A. Abd El-Latif · Xiamu Niu., 2013,"New approaches for efficient information hiding-based secret image sharing schemes", DOI 10.1007/s11760-013-0465-y.

[21] Bala Krishnan Raghupathy et. al., 2014, "An Enhanced Bishop Tour Scheme for Information Hiding", Volume 9, Issue:1, pp: 145-151.