International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 10 (2015) pp. 25501-25510

http://www.ripublication.com

A New Steganographic Technique Using Combination of EEE and DDE

[1]Manish Grover, [2]Pushpendra Kumar Petriya, [3]Sandeep Tripathi

1 sachinmanish78@gmail.com1 Student, Lovely Professional University, India
2pushpendra.14623@lpu.co.in2Assistant Professor, Department of CSE, Lovely Professional University, India.
3sandeep.tripathi@amdocs.com3Data Warehouse Group Leader, Amdocs DVCI

Abstract

This paper proposes a new steganographic techniquewhich is a combination of EEE and DDE which uses Qr-code image created for encrypted text using symmetric algorithm and hiding into cover image. As we know that steganography combined with cryptography provides security as well as a level up by hiding its existence. We are using advanced encryption standard (AES) to encrypt the text with a key at sender's end and that text will be decrypted at receiver's end by same key shared privately. Sender is transferring a sego image to receiver it is created using least significant bit (LSB) technique. The proposed technique provides good hiding capacity, cost effectiveness, reliability and higher security as compared to other symmetric algorithms as the results shown are good which proves that algorithm provides security at two level first at the time of encryption of text and second while concealing of qrcode into cover image for hiding existence of the text embedded.

Keywords: Steganography, AES, LSB, Qr-code, EEE, DDE.

1.Introduction

In the world of insecurities where we are surrounded by the many problems related to our privacy whether it's our personal life or professional comes a major part which is played by us for our organization. Working as a part of an organization requires commitment and devotion to meet the demand for robustness and high-performance. Today in this era of Internet where every second a new device is attached either smart devices or laptops introducing new identities sharing their information by either using social networking websites or applications on hand-held devices.

At this time today no one has time they want work to be executed fast and efficiently without compromise they want every functionality of high end devices on their smart-phones and tablets like Editing documents and pictures, making presentations etc. seeing this growth rate companies have modified their standard of working for end devices and are now in race for achieving higher values in mobile devices every company is now interested in working for mobile devices as market has turned monopolistic towards handheld device application development as it is clear that edge of tomorrow lies in developing for most common daily use device which has effected people's life to such an extent that they could not bear any second without their devices and as modern technology is taken control over and have adjusted in an important place in everyone's life.

With this comes everyone's first priority that is privacy including CIA traits within security which is related to either a person or an organization for which they work. Compromise of security can leads to devastation of the company or organization thus this threat security leads to new area of work which require special kinds of skill and knowledge of techniques like changing real form of text by encoding at Sender's end and Decoding at Receiver's end so its real form is undetectable using symmetric and asymmetric Algorithms in presence of third party. These symmetric and asymmetric Algorithms were given under a category today known as cryptography which is also seen as "black art".

Cryptographic algorithms work for CIA traits especially for authentication and authorization as an authorized person having key can authenticate itself and decrypt the coded message or data send by other person. Alone cryptography provides encryption decryption mechanism with hashing techniques to change content form using some mathematical logics and algorithms. Due to extensive use of these algorithms for past few years these have become more open and public.The steganography aims to prevent a third party fromgetting to know that any covert communication has taken place which is better than theencryption. It is defined as the art and science of hiding information, transmitting secretmessages through innocuous cover Media Carriers in such a manner that the existence ofembedded messages is undetectable. Only persons who have knowledge of the embeddedinformation and possess a"key" will be able to decode and view the information. The key used can take many forms. It could range from a passphrase for electronic steganographyto an understanding of a method to decode the information.

The aim of this paper is to propose a simple and reliable approach for two people or organizations to contact securely without fuss and share private data easily over internet without caring about any third person which might be monitoring their network to get some of the valuable information for intruding in their network and provide any type of harm to the people or the organization for which they are working. In this paper we are proposing a LSB technique for first time using color images as every other researcher has proposed their techniques for grayscale images and we are using Qr-code to hide existence of encrypted data and encryption using most secure symmetric algorithm AES and handling they key directly to the receiving party.

1.1 Steganography

The primary motivation behind steganography, which signifies 'Writing in hiding' is to conceal information in a spread media so others won't have the capacity to recognize it. While cryptography is about securing the substance of messages, steganography is about disguising their extremely presence. The applications of data concealingframeworks for the most part range over an expansive territory from military, Discernment organizations, online decisions, web keeping money, restorative imaging and so on. These mixture of uses make steganography a hotly debatedissue for study. The spread medium is ordinarily pickedremembering the sort and the measure of the mystery message and numerous diverse transporter document arrangements can be utilized. In the current circumstance advancedpictures are the most well-known transporter/spread recordsthat can be utilized to transmit secret data.

Terminology

Cover image and message are two terms composed in Steganography. Cover image is the carrierthat hides message which is the secret data that needsto be hidden.

Fig.1: Data Hiding Scheme*[6]*

1.2 Cryptography

Cryptography is a technique for putting away and transmitting information in a structure with the goal that it can no more be translated or caught on. It is a study of ensuring viable method for securing delicate data as it is put away on media or transmitted through system correspondence ways.

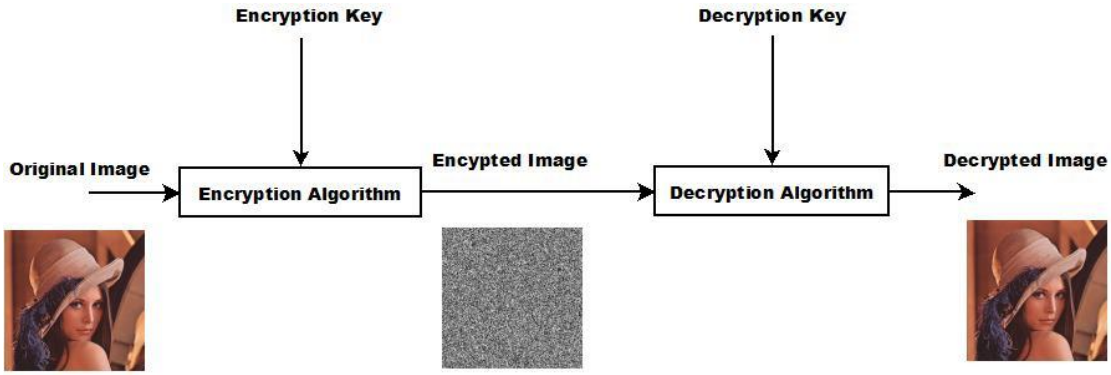

Fig.2: Data Encryption-Decryption Scheme

1.3 Qr-Code

Quick Response Code a trademark for a type of matrix barcode firstly designed to be used by an automotive industry in Japan.

A Qr-code is an optical machine–readable label that contains data about the item to which it is attached. The Qr-code system has become most popular nowadays they are bounded for automotive industry due its exciting features which are fast readability and having higher capacity storage as compared to UPC barcodes. Talking about its applications which include tracking product, identifying item, managing documents tracking time and most of all general marketing.

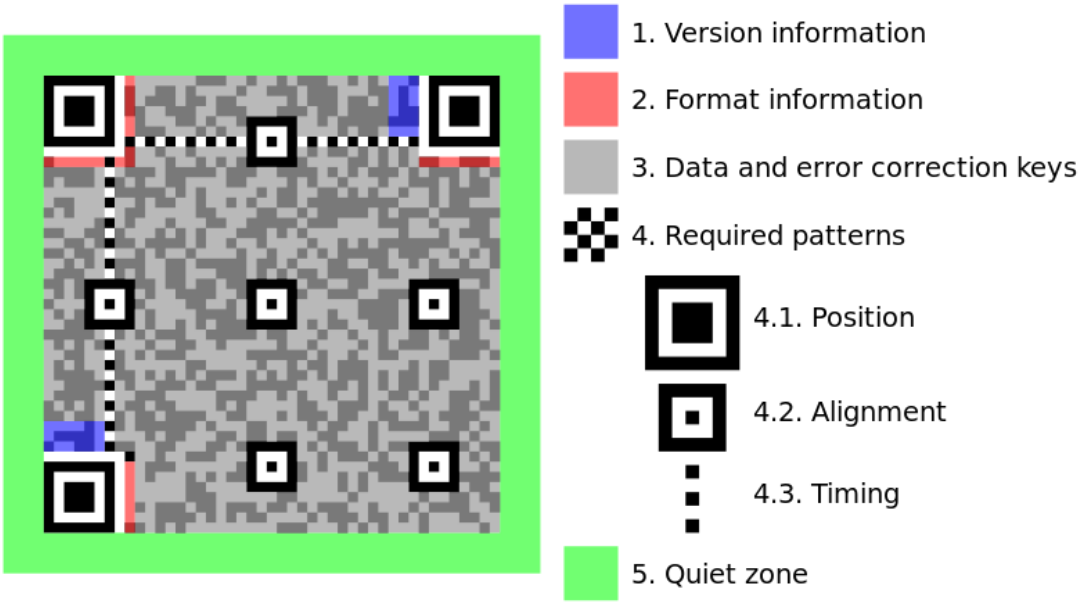

Fig.3: Standards of QR Code [7]

In further sections, Section2 is for Literature Review, Section 3 is for proposed system, Section 4 is for Results and Discussion and ending with Section 5 is for conclusion.

2. Literature Review

In 2007 Sanjay Kumar Jena and G.V.V.Krishna proposed another recognition calculationwhich diminish startingbias,and approximated LSB Embedding messageproportions bybuilding mathematical statements with measurements which is an upgraded algorithm tothe distinction picture histogram algorithm and performed tests on a gathering of unaltered lossless pictures. Their Experimental results demonstrate that this calculation is more precise and solid than that of ordinary distinctionpicture histogram strategy. The algorithmdiminishes the mean slip by 50% for implanting proportions more prominent than 40%when contrasted with the Difference Image Histogram Algorithm.[1]

In 2009 Venkata Abhiram.m et. al's. article , the essayists propose a randomization framework that makes usage of RGB estimations of shading pictures to enhance unclearness. In the three channels RED, BLUE, GREEN the LSB of any of the 3 channels is used as an issue to pick introducing breaking point in the other two channels. In the randomization strategy, the LSB of any of the channels (RGB) are used to show how data must be concealed in the staying 2 channels. In case the last two bits of the channel are 00 there is no covered data, if it is 01 embedded just in channel 2, if it is 10 data is introduced in direct 1 and if it is 11 data is embedded in both the channels. Three methodology are used.[2] They are

- RED is utilized as default pointer.
- Client chooses any channel as pointer.
- Pointers are picked focused around a cyclic arrangement and information is installed.

In 2009 Jasvinder Kaur et.al's.the writers examine diverse steganographic systems taking into account computerized rationale and proposes another upgraded steganographic strategy focused around it. The transporter picture is chosen relying upon the data to convey. This procedure utilizes computerized operations focused around rationale doors and movement administrators to insert/get the concealed data from picture information. Contingent upon the span of the data to implant the transporter picture is partitioned into lines and information is implanted utilizing computerized operations.[3]

In year 2014 Divyasukhija gave a review on certaincryptographic algorithms author hasdiscussed about two techniques AES (Advanced Encryption standards) and DES (Data Encryption Standards) where in author reviewed these algorithms in details. Author has givenimportant facts about symmetric as well as asymmetric algorithm and has briefly shownhow and why we are using such kind of algorithm. Author has told about brief the historyof DES and AES and has also discussed Strengths and Weakness for the same.[4]

In 2013 Yu-Hsun Lin et.al's presented a systematic framework for QR code beautification. They integrated visual saliency consideration seamlessly with simulated annealingoptimization. They have created framework in order to remove the shortcomings of noise-likelooks of QR codes. It is seen since QR code has already been ubiquitously utilized in the mobile computing era, for higher impact the beautification ofQR code is a problem. Their work can greatly enhance the aesthetic perception of QR codes for users.[5]

3. Proposed System

The system proposed in this paper uses encoding and embedding and decoding and extraction procedures with different techniques.

1. Encryption using AES + Encoding Using QR-Code + Embedding using LSB Technique.

This algorithm is used at sender's side firstly sender encrypt the message using a

private key using AES as the encryption algorithm and then that encrypted text is passed to QR-Code encoder where that encrypted message gets its first layer of protection and then we get a QR-Code containing the encrypted message which is taken famous compression format either .jpg or .png which will be afterwards embedded in the

Cover image using another well-known technique and famous in steganography the LSB technique to create a stego-image and then it is send to the receiver.

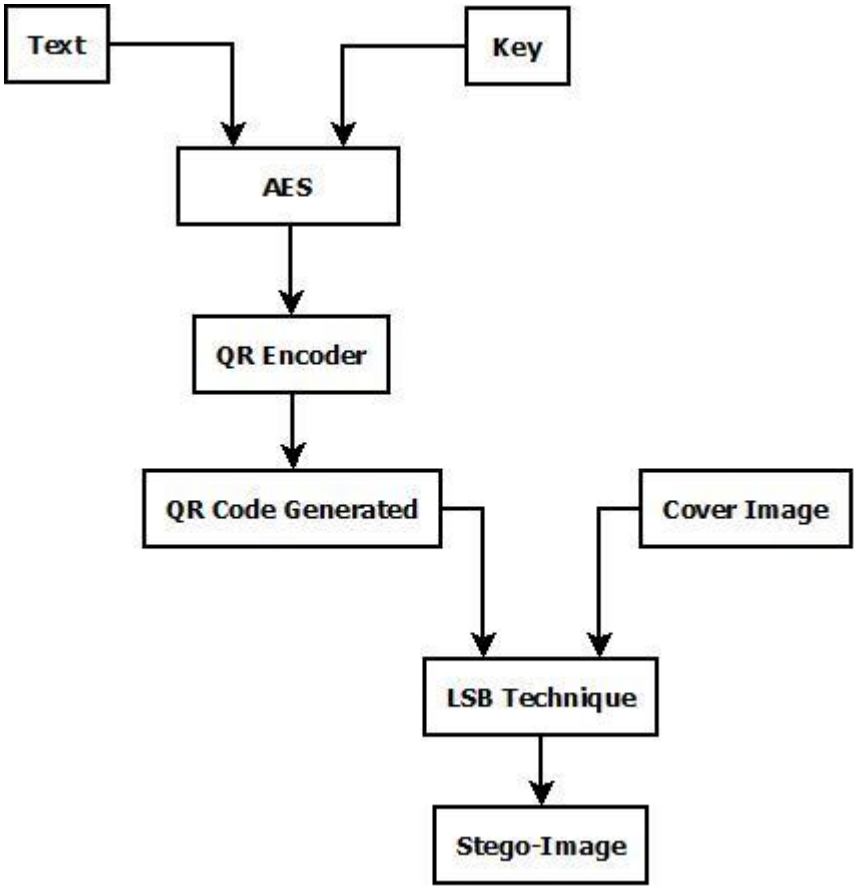

Fig.4: EEE Algorithm

Proposed EEE (Encryption, Encoding, Embedding) Algorithm:

1. Text: The Message to be encrypted.
2. Key: The key will like a password to open the encryption lock to see the message. As we are using symmetric algorithm so this is to be shared personally with the receiving party.
3. AES: Advance Encryption Standard technique with fixed block size of 128 bits and variable key sizes of 128 ,192 or 256 bits. It is designed on the principle as substitution-permutation network and is fast in both software as

well as hardware.

4. QR Encoder: We have used most popular zxing (zebra-crossing) library to create the encoder.
5. LSB Technique: The most established system for concealing the message in an image using the LSB Technique. In LSB Technique we hide the message at all least used set of bits (LSB's) of pixel estimations of an image. In this method binary equivalent of the secret message is distributed among the LSBs of each pixel.
6. Stego-Image: Final image which will be send to receiver at the communication medium.

2. Decryption Using AES + Decoding of QR-Code + Extraction using LSB Technique.

This algorithm is used at receiver's side firstly receiver extract cover image and QR-Code from the stego-image and then encoded message is decoded using QR-Code decoder and then encrypted message is passed to AES system and with help of same private key which only the authorized receiver have can decrypt the message and read it.

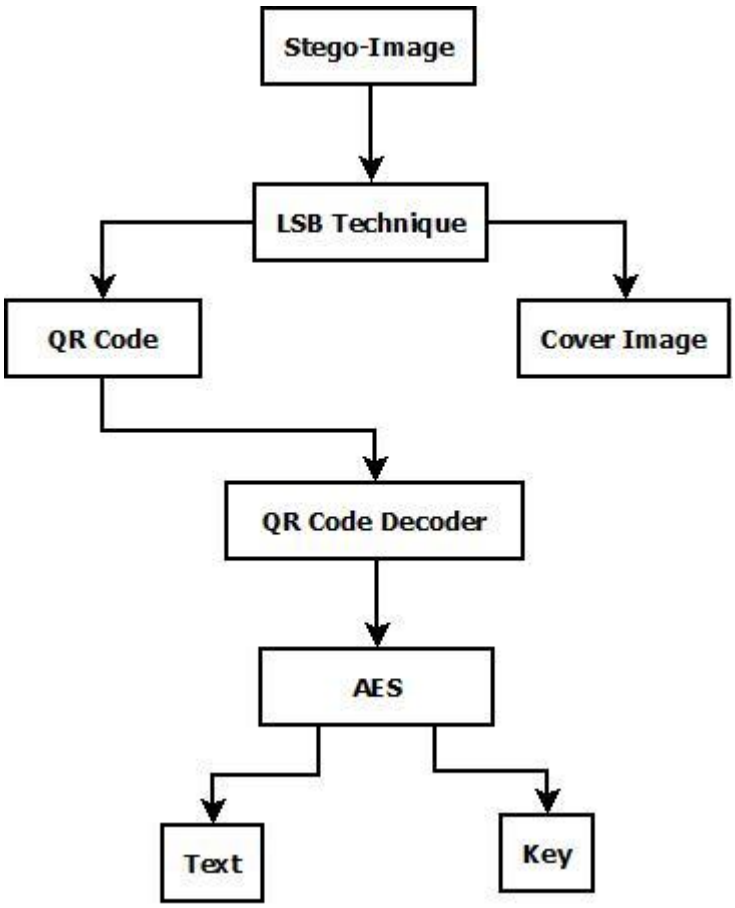

Fig.5: DDE Algorithm

Proposed DDE (Decryption, Decoding, Extraction) Algorithm:

1. QR Decoder: We have also created the decoder using zxing library.
2. Key: Same key will be used at the time of decryption.

4. Results and Discussion

In this section, the proposed system results have been discussed.

We have tested results for certain images

1. Cover Image: This Image is like cover of letter which is to hide existence of the letter as well as to secure the image and with same phenomenon we are hiding and securing our secret message embedded QR-Code image.

Fig.6: Our Cover Image

3. QR-Code Image: This Image is very precious part of our proposed algorithm which contains our secret encrypted message.

Fig.7: QR-Code Image

4. Stego Image: This is the image which will be send to receiver and which is created by combining cover image and the image to embed.

Fig8: Stego Image

Parameters taken for results

1. **PSNR:** -Peak Signal to Noise Ratio it is the ratio of square value of pixels by MSE expressed in decibel. It

Measures the statistical difference between stego-image and cover image and can be calculated using given equation.

$$PSNR = 10log_{10}\frac{255^2}{MSE}\text{db}$$

2. **MSE: -** Mean Square Error it is the square of error between stego-image and cover image. MSE measures distortion of image and calculated using the given equation.

$$MSE = \left[\frac{1}{M * N}\right]\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X_{ij} - X'_{ij}\right)^2$$

Where:
Xij: The intensity value of the pixel in the cover image
X'ij: The intensity value of the pixel in the stego image.
M ∗**N**: Image Size.

3. **Time:** This is find the time taken for embedding and stego-image formation in seconds.

Table 1: PSNR, MSE and Time values

Cover Image	PSNR	MSE	Time
100.jpg	41.5105	9.20718e+08	2.28284
Sheep.png	42.2732	8.71757e+08	1.00553
Kola.png	40.2283	6.85342e+08	1.05313
Lena.jpg	42.8694	1.25897e+09	0.938499
Plane.png	45.4658	2.28907e+09	0.4308795
106.jpg	44.3031	1.75144e+09	1.41246

5. Conclusion

As we have seen that results of our proposed algorithmmeet their every objectives hence it is for color image opening anew field to work with newtechnologies our proposed algorithm works on both color as well as gray-scale images we have tested results for many images of different size but we have shown for two sampleswith different dimensions thus it also provide good speed as it is tested on a single system but values may depend on systems configurations and memory.In future this algorithm canbe integrated with optimization algorithms and can be used for 3D as well as 4k images.

References

1. S. K. Jena and G. Krishna, "Blind Steganalysis: Estimation of Hidden Message Length," *International Journal of Computers, Communications & Control,* vol. 2, no. 2, pp. 149-158, 2007.
2. V. Abhiram.M, S. Imadabathuni, U.Padmalochini, M. Imadabathuni and R. Ramnath, "Pixel Intensity Based Steganography with Improved Randomness," *International Journal of Computer Science and Information Technology,* vol. 2, no. 2, pp. 169-173, 2009.
3. J. Kaur, I. Duhan and M. Duhan, "A Comparative Analysis of Steganographic Techniques," *International Journal of Information Technology and Knowledge Management*, vol. 2, no. 1, pp. 191-194, 2009.
4. D. sukhija, "A Review Paper on AES and DES Cryptographic Algorithms," *International Journal of Electronics and Computer Science Engineering* , vol. 3, no. 4, pp. 354-359, 2014.
5. Y.-H. Lin, Y.-P. Chang and J.-L. Wu, "Appearance-Based QR Code Beautifier," *IEEE TRANSACTIONS ON MULTIMEDIA,* vol. 15, no. 8, 2013.
6. C.P.Sumathi, T.Santanam and G.Umamaheswari, "A Study of Various Steganographic Techniques Used for Information Hiding," *International Journal of Computer Science & Engineering Survey,* vol. 4, no. 6, 2013.
7. D. Gthberg, "QR-Code," 12-5-2014. [Online]. Available: www.wilkipedia.org/QR-Code. [Accessed 12- 5- 2014].