ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 3 , March 2016

Visual Cryptography Scheme for Secret Image Retrieval

Monika Bhosale , Rajshree Chaudhary , PrathameshGaddam, AyushiKedar
Yogesh. J.Pawar

Student, Department of Information Technology, NBNSSOE, SavitribaiPhule Pune University, Pune, India
Student, Department of Information Technology, NBNSSOE, SavitribaiPhule Pune University, Pune, India
Student, Department of Information Technology, NBNSSOE, SavitribaiPhule Pune University, Pune, India
Student, Department of Information Technology, NBNSSOE, SavitribaiPhule Pune University, Pune, India
Professor, Department of Information Technology, NBNSSOE, SavitribaiPhule Pune University, Pune, India

ABSTRACT: In multimedia system, first the message will encrypt and then it will hide into an image file. So that we can use Cryptography because this can converts the message into an unreadable text. These both provide the security over the unsecured communication channel. Cryptography technologies are high secured system. These features of cryptography and stenography of data hiding are combined to visual cryptographic steganography technology. The visual cryptography (VC), is a (t,n) secret stacking of t-1any transparencies which reveals the sharing scheme where a secret image is encoded into transparencies, and the image is obtained. The stacking technology is used to extract any form of information secret. This can be used two transparent images. Among these images, one image can use for random pixels and the second contains secret information. It is unfeasible to get the secret information with the images. To get the secret information, both images are used. In this proposed scheme allows to dynamically changes including new transparencies without distributing the original transparencies. In this project the system divides the images and message in to two parts such as Key and Cipher, which means transparency and printed page. Such as both are consider as a separate then they are random noise but the combination of an image and message was first encrypted.

KEYWORDS: Visual Cryptography (VC), Secret Sharing, Random Grids (RGs), Bit Plane Complexity Segmentation (BPCS), Universal Unique Identifier (UUID).

I. INTRODUCTION

Visual cryptography is nothing but the secret sharing. In the Visual cryptography a secret image can encoded into the transparencies that means key, and the transparencies can connect with the noise-link so that the information cannot be use by using any other transparency. In general, a (t,n) VC has the following properties: The VC generated transparencies can reveal the secret by visual perception, but the stacking of any t-1 or the number of transparencies cannot use any information according to the size of the secret image [1]-[2]. Contrast is important performance metrics for VC. In general, the stacking revelation of the secret with the better visual quality, and therefore the stacking secret with high contrast is the VC designs.

How visual Cryptography works:

The image can be divided into each pixel of smaller blocks. There are some white and black blocks. In this each pixel can divided into four parts, there two white and two black blocks.In the table on right we can see that a pixel, which is divided into four parts, which is having six different states. If the pixel on a layer 1 has a given state, the pixel on the layer 2 may contain two states: 1st is the identical or inverted to the pixel of layer 1.If the layer 2 is similar or identical to layer 1,thenthe overlaid pixel of layer will be half black and half white. If the pixel of layer 1and 2 both is opposite, then the overlaid version will be completely black [3]. This is nothing but the information pixel. In this table we have the two layers.

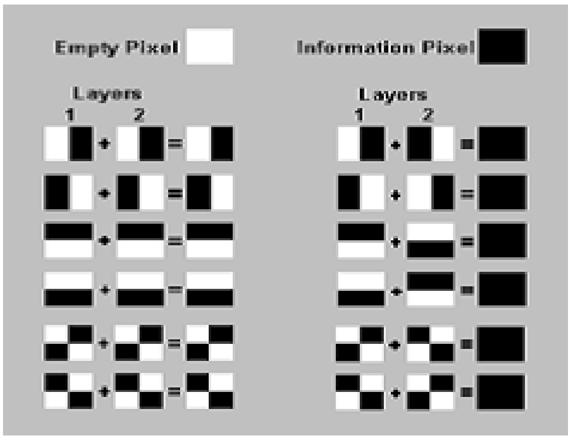

Figure 1: 2 out of 2 scheme (4 subpixels)

One is the transparent image, in layer 1, has which all have a random state, with random state, having six possible states. In this layer 2 is identical to layer 1, expect the black pixel when overlaid, so the area looks like grey, and the opposite area will black. In this system the pixel can applied in different ways.

II. LITERATURESURVEY

- There was a demonstration of a visual secretsharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. There are several generalizations of the basic scheme including k-out-of-n visual cryptography.

- A low-cost and simple technique for encryption of two-dimensional patterns and shapes is suggested and demonstrated[6]. The method is based on the superposition of random grids. A binary secret image in this system is encoded into two noise-like transparencies[4] with the same size of the original secret image, and stacking them content of the secret. Comparing RGs with basis matrices, one of the major advantages is that the size of generated transparencies is unexpanded.

- Two implementations are based on the above principle. The first shows how keys for encryption can be randomly generated by the transmitter, without the necessity of exchanging them with the legitimate recipient. The keys are ‘embedded’ in a master key and are recovered from it by the intelligence of the legitimate recipient after he or she uses the master key. No human intelligence can be helpful to a user who does not posses the master key. The second implementation concerns the possibility of creating a secret connection between a numerical key and a specific image. Such a scheme can be used, for eg , in validating the identity of the users of credit cards. The possibility of integrating human visual intelligence into the process of encrypting sensitive information by presenting certain visual information to the recipient’s eye is discussed. This adds a new dimension to the crypto complexity of such a process.

III. PROPOSED SYSTEM

In this project we can implement the key using encryption and decryption. In text format it can encrypt first and then it is decrypted using the key. Also we can work on image as shares. The image is divided into 2/2,2/3,2/4,2/5,3/3,3/4,3/5,2/2-grey,2/2-coloured[6],2/2-with same random/key,2/3-with general access shares. Each share is stored in the desired destination and then each share is encrypted. These shares are then sent to the sender for decryption. After receiving by the receiver, these shares are first decrypted and then overlapped in order to obtain the final image. The final image cannot be obtained until and unless all the shares are overlapped. In this implementation we can use key for security, because by using key only sender and receiver knows that the key as well as the encrypted or decrypted message. In this encryption and decryption process the message can be encrypted in an image format and during decryption the message can be viewed by using the key which is send by the sender. In this system we can include one step for security, we can send the text using key and in that key we can add the folder name during encryption time, then it generates one single key and during decryption process we can use this key and folder name when we use this folder to get the original text.

IV. ARCHITECTURE

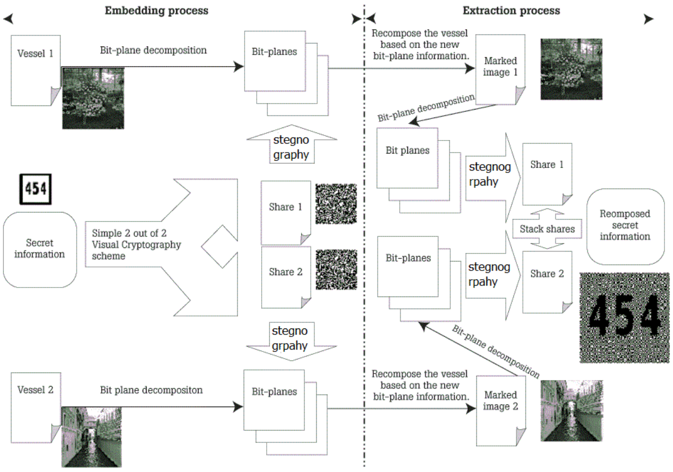

Figure 2: Architecture of visual cryptography scheme for secret image retrieval

In Figure 2 in the embedding process the secret information is carried using a 2 out of 2 visual cryptography scheme[8], the image is divided into 2 shares each share is embedded[5] using a BPCS. The shares are then encrypted and a unique key is generated, the key is then sent by the sender using steganography to the receiver. The receiver then uses the received key to decrypt the encrypted shares in order to obtain the original data[7] In the extraction process, the bit planes recompose the image based on the new bit plane information which is then water marked, the marked image again undergoes bit-plane decomposition where new bit-planes are created which are then extracted based on BPCS which gives two shares in the stack of shares and then recomposed to the secret image/message.

After this the encryption process begins where the key is assigned which undergoes AES algorithm (128 bits). The algorithm then gives a cipher text which is the encrypted data. To decrypt the data again the algorithm is used with the key assigned initially to get the plain text or original message back.

Algorithm:

Cipher text algorithm:

A plaintext is a fixed length part. In this paper, an encryption algorithm which encrypts the first part of the plaintext and the key of the second part to a cipher text is proposed. Basic computing operations, such as inserting dummy symbols, rotating, transposition, shifting, and complementation, are applied to encrypt plaintext to cipher text. It is secure for the cipher text transmitted through the network since the tables of cipher text are produced randomly and it is difficult to carry out cryptanalysis.

Pseudocode:

```
INPUT: plaintext x,key K

OUTPUT:ciphertext y = eK(x)

ASSUMED: round function g, last round h,key scheduling procedure giving Ki, ciphertext y, encryption function e, Number of times intermediate ciphertext repeated Nr

w0 = x

fori = 1 to Nr −1

wi = g(wi−1, Ki) y = g(wNr−1, KNr−1)
```

Random alphanumeric string algorithm:

This algorithm works by choosing 130 bits from a cryptographically secure random bit generator, and encodes them in base 32. 128 bits is considered to be cryptographically strong, but each digit in a base 32 number can be encoded 5 bits, so 128 is rounded up to the next multiple of 5. This encoding is compact having 5 random bits per character and also efficient. Compare this to a random UUID, in standard layout it has only 3.4 bits per character, and only 122 random bits in total.

If you allow session identifiers to be easily guessable (i.e. too short, flawed random number generator), attackers can hijack other's sessions. Note that Secure Random objects are expensive to initialize, so you'll have to keep one around and reuse it.

Here is alternative code for cheap, by insecure random alpha-numeric strings. You can tweak the "symbols" if you want to use more characters.

AES Encryption:

AES is a cheap and uncomplicated technique for encryption of two-dimensional patterns and shapes is suggested and demonstrated. A binary secret image in this system is encoded into two noise-like transparencies with the same size of the original secret image, and stacking them content of the secret. In this project, AES encryption has input character of 16 byte. Cipher text class is used for both encryption and decryption. Certificate of cipher text generates the public key in bytes. doFinal() method is used for key updation.BASE64Encoder reads the updates key and encrypts the sender key.

AES Analysis

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES have been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of ‘future-proofing’ against progress in the ability to perform exhaustive key searches.

However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

Decryption Process

Visual cryptography is that current space of analysis wherever heap of scope exists. There are various innovative ideas and extensions exist for the basic visual cryptographic model introduced till now. In the existing VC schemes[8] no security is provided to the secret shares and intruder can alter its bit sequences to create fake shares. In this paper we provides higher levels of security to the information being transmitted so that the intruders cannot easily break the system. Even if they realize the existence of a secret data they cannot easily recognize the data, since data is hidden. Firstly the encrypted cipher text is provided for decryption. In the cipher text, the username and the key is split using the term "split". If the username provided is correct then only true results would be returned. Later the key provided for decryption is read by the system if correct then only the plain text can be obtained back.

V. FUTURE SCOPE

- It exploits human eyes to decrypt secret images with no computation required.
- XOR operation so, computation is easy.
- Generation of infinite number of shares dynamically.

VI. CONCLUSION

Finally we conclude that the original text can be secure as possible using key. Key can be generated using some algorithm. In the Encryption process we can use key and folder name and generate one key for encryption. In the process of decryption we can use this key and get the key and folder where the text have saved, then we use the folder to get the original message. Also in this project we can use image which is divided into shares into 2/2.Also the text message can be encrypted and decrypted using the key. So this project is very secure for sending and receiving the message.

REFERENCES

[1] Adi Shamir, How to share a secret. Communication of ACM, Volume 22, No. 11, Pages 612-613, 1979.
[2] M. Sukumar Reddy, S. Murali Mohan, Visual Cryptography Scheme for Secret Image Retrieval, IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.6, June 2014.
[3] W. Gandhare P. S. Revenkar, Anisa Anjum, Survey of visual cryptography schemes. International Journal of Security and Its Applications, Volume 4,No. 2 pages 49-56, April 2010.
[4] C. N. Yang, “New visual secret sharing schemes using probabilistic method,” Pattern Recognit.Lett., vol. 25, pp. 481–494, Mar. 2004.
[5] K. Braun and R. L. de Queiroz, Color to Gray and Back: Color Embedding Into Textured Gray Images, Proc. IS&T/SID 13th Color Imaging Conference, pp.120-124, 2005.
[6]Young-Chang Hou, “Visual cryptography for color images”, Pattern Recognition 36 (2003), 1619-1629.
[7] Tzung-Her Chen and Kai-Hsiang Tsao, “Visual secret sharing by random grids revisited”, Pattern Recognition, 42(9):2203 - 2217, 2009. Elsevier Science Inc. New York, NY, USA.
[8] Debasish Jena, Sanjay Kumar Jena, “A Novel Visual Cryptography Scheme”, International Conference on Advanced Computer Control, 2008.