VISUAL CRYPTOGRAPHY SCHEME FOR COLOR IMAGE USING K-N SECRET SHARING ALGORITHM

Prof. Sujit Ahirrao[1], Tusharkumar Sakariya[2], Abhijeet Bhokare[3], Rahul Thube[4]

[1]Assistant Professor, Computer Engineering, [2, 3, 4] Computer Engineering

Sandip Institute of Engineering & Management, Nashik, (India)

ABSTRACT

Visual cryptography is a powerful encryption technique which is used to secure image base private data that can be decrypted using human visual system (HVS).The cryptography system encrypts the image, and that image is divided into n shares, and decryption is done using k number of shares. The existing technique that is simple visual cryptography is not much secure because decryption process is done using human visual system. If any user at least get k number of shares that secret information can be retrieved. Watermarking is a technique which puts a signature owner within a creation. In this project work we have proposed secure visual cryptography scheme for color images where the number of shares (n) that are divided and enveloped in other images using invisible digital watermarking. Shares are generated using random number generator.

Keywords: Digital Watermarking, K-n secret sharing, Random sequence, Visual Cryptography scheme.

I. INTRODUCTION

Visual cryptography is nothing but a cryptographic technique where as information like Image, text, etc .That are encrypted in a way that the decryption technique can be performed by the human visual system. Like another multimedia components, image is sensed by the person. Pixel is nothing but the smallest components constructing a image. Each pixel is made of a 32 bit digital color image. Images is divided into four parts that are following.

1. Alpha
2. Red
3. Green
4. Blue.

A 32 bit pixel is represented in the following figure [11][14].

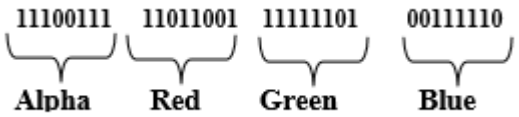


Figure 1: Structure of 32 bit pixel

Each is made of 8 bits. Alpha part is representing the degree of transparency. Visual system is acts as an OR function. Two transparent objects are get together and produced the transparent object. If changing any of them

to non-transparent, then final objects will be seen as non-transparent. In visual cryptography scheme, k-n secret sharing algorithm an image is divided into n number of shares and such that minimum k number of shares are taken to reconstruct the original image. The division can be done by using Random Number generator. This type of visual cryptography technique is not much secure as the reconstruction is done by using simple OR operation. We are adding more security to visual cryptography scheme we have proposed a technique called digital enveloping.

This is nothing but an digital watermarking technique.

Using this technique, the number of divided shares are produced by k-n secret sharing visual cryptography scheme. that shares are embedded into the envelope images by using LSB replacement. The color changing of the enveloped images that are not sensed by human eye (there are more than 16.7 million i.e.224 different colors that are produced by RGB(Red, Green, Blue) color model. So human eye can see only a few of them).Because they are not visible. This technique is known as digital watermarking because human eye cannot see the change into the enveloped image and the enveloped (Producing after LSB (least Significant Bit) replacement) image. In the decryption process k number of shares are embedded into envelope images that are taken and LSB replacement are retrieved from each of them done by using OR operation to generate the source image. The Overall process of project is describes in later part of project. The process of k-n secret sharing Visual Cryptography scheme on the image are described, also describes the enveloping process using digital watermarking, decryption process, the expected result, and Alpha, Red, Green and Blue, also draws the conclusion.

II. LITERATURE REVIEW

In this chapter we will see various studies and researches conducted in order to identify current scenarios and trends in hiding the images using visual cryptography. In literature Survey we are going to study 3 Existing systems which are use in Visual cryptography system. These Systems are:

2.1 Shamir's Secret Sharing Scheme

The Shamir's secret scheme divides a secret data S into n number of shares let be S1, S2. . . . . Sn. such that

1. Values of k or more shares among Si (i n) can retrieve the secret information.
2. Values of less than k shares retrieve no information about the secret share.

This type of technique is called (k, n) secret sharing algorithm. This technique is described with an example in the following parts. The (k, n) secret sharing comes from the concept that k number of points are necessary to define a polynomial of degree (k=1). To construct the polynomial, (k=1) coefficients a1, a2. . . . ak=1 are needed.

Here a0= S, the secret data. The polynomial f(x) = a0 + a1x +

a2x2 + ...+ak=1xk=1 is constructed from the coefficients. Total n points i.e. let I = 0. . . ..n are taken and corresponding f(x) are also be calculated. From values n number of pairs (i, f(i)) are constructed. The original coefficients can be retrieved by interpolation method from at least k numbers of these pairs[11].

2.2 Blakley Secret sharing scheme

Blakley secret sharing is based on hyper plane. It is a true that non-parallel lines intersect at a specific point [5]. This secret sharing scheme says that,

1. Secret is point is must in m-dimensional space.
2. Share corresponds to only a hyper plane.

3. Intersection of threshold planes gives the secret values.

4. Less than threshold planes will not intersect to the secret values.

2.3 Asmuth-Bloom secret sharing scheme

This technique is based on Chinese Remainder theorem[5]. This technique takes a sequence of pair in co prime integers p0, p1, ... pn such that where n > 2 and 2 k n. The working principle of this scheme is as following:

1. The secret S is chosen as a random element from the set Z.

2. A random integer a is chosen such that S + ap0 < p1p2. . . .pk.

The reduction modulo mi of S + ap0 for all 1 i n are calculated. These are represents shares i.e. following. Ii = (Si, pi).

3. From given k distinct shares Ii1 , . . . , Iike, the following set of equations are formed As pi1, pi2, ...pik. The secret S is the reduction module p0 of S0[5].

Recently in the literature, many new methods have been implemented for visual cryptography. In 1994 Naor and Shamir [11], have developed the Visual Secret Sharing Scheme (VSSS) to implement this model [11]. In the previous system called n-n sharing visual cryptography scheme, the image can be retrieved even if only k shares are available, this is a major security issue. In our proposed system, the image can be retrieved only if all n shares of images are available. Apart from this, we use random number generator for generating shares of images. From above Literature survey, we found some limitations & drawbacks of visual cryptography using complex number system that it does not provide more security to organization & it Uses complex number algorithm for black and white images. Proposed System will provide the random number for encryption and decryption. It also uses digital watermarking for security purpose.

III. METHODOLOGY

Step 1: The source image is divided into n number of shares using k-n secret sharing visual cryptography scheme such that k number of shares is sufficient to reconstruct the encrypted image.

Step 2: Each of the n shares generated in Step 1 is embedded into n number of different envelope images using LSB replacement.

Step 3: k number of enveloped images are generated in Step 2 are taken and LSB (least Significant Bit) retrieving with OR operation, the original image is produced.

IV. MODULES

4.1 K-N Sharing Visual Cryptography Scheme

The source image is divided into n number of shares using k-n secret sharing algorithm visual cryptography scheme such that all n number of shares are needed to reconstruct the secret image. In this module, a method for random number generation is used to generate random number shares of the secret image.

4.2 Encryption Module

In this Module Using this step the divide number of shares of the original image are enveloped within other different image. Least Significant Bit (LSB) replacement using digital watermarking is used for this enveloping process. It is already discussed that a 32 bit digital image pixel is divided into four parts that are following,

1. Alpha

2. Red

3. Green

4. Blue

Each bit made of8 bits. Experiment shows that if the last two bits of each of these parts are changed, then the changed color effect is not visible by human eye. This overall process is known as digital watermarking.

4.3 Decryption Module

In this step all n numbers of enveloped images are considered as input. Where each of these images for each pixel, the last two bits of alpha, red, green and blue (RGB) are retrieved and OR operation is performed to get the original image. The logic is that human visual system is acts as an OR function. For generated process; the OR function can be used for the case of stacking n number of enveloped images.

This three modules are shown in above figure.

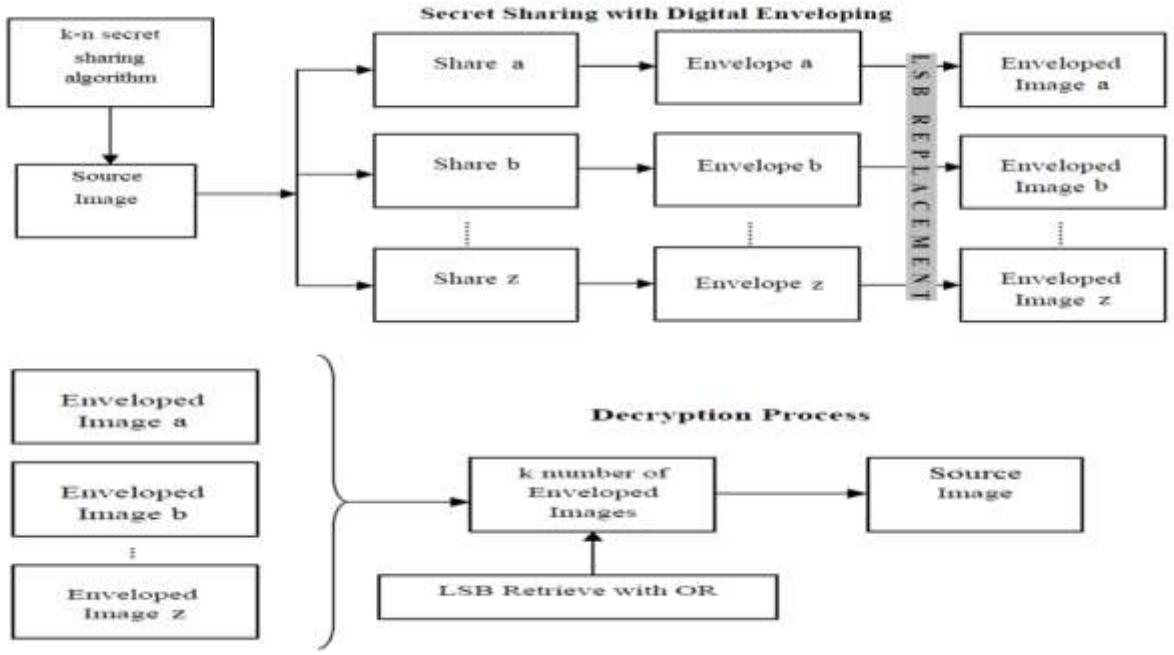


Fig 2: Block diagram of modules

V. EXPERIMENTAL RESULT

5.1 Division Using Visual Cryptography

Source Image: parrote.png

Source Image is

Fig: Source Image

Number of Shares:4

Number of shares to be taken:3

Image shares produced after applying Visual cryptography are:

0img.png

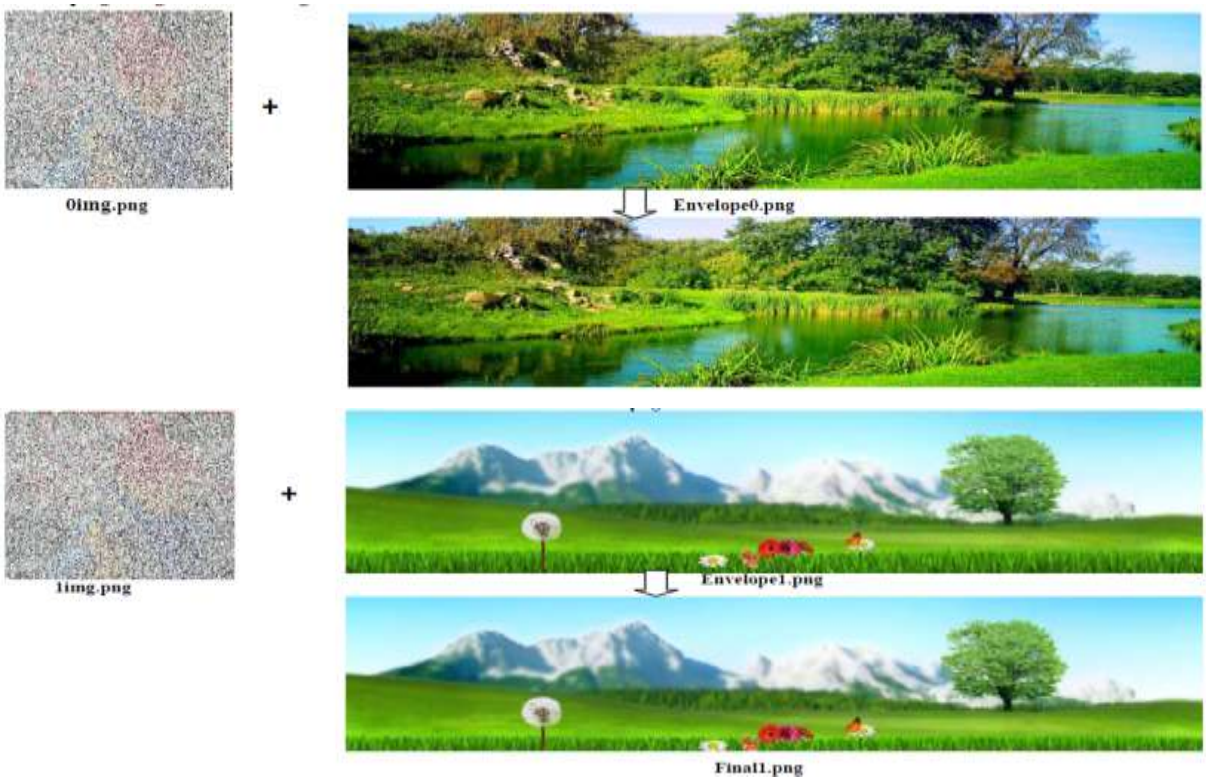
1img.png

2img.png

3img.png

Fig:Encrypted Shares

5.2 Enveloping Using Watermarking



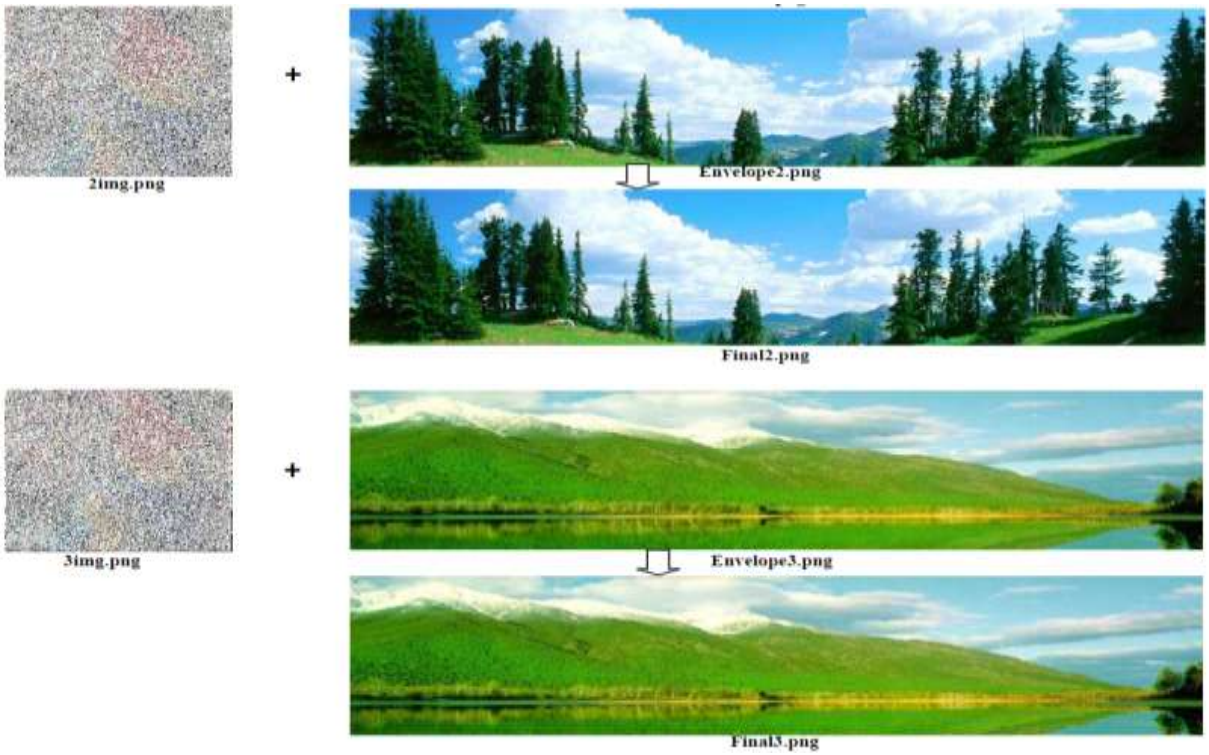


Fig: Enveloping shares using digital Watermarking

5.3 Decryption Process

Number of enveloped images taken:3

Name of the images : Final0.png , Final1.png , Final2.png

Fig: Decryption Process

VI. CONCLUSION

Decryption part of visual cryptography algorithm is based on OR operation, so person gets sufficient k number of shares. The image can be easily decrypted using k-n secret sharing algorithm. In this work, with well known k-n secret sharing using visual cryptography scheme an enveloping technique is used where the secret shares are enveloped within images using Least Significant Bit replacement digital watermarking. This providing security to visual cryptography technique from malicious attack.

REFERENCES

[1] International Journal of Scientific and Research Publications, Volume 3, Issue 3, March 2013 1 ISSN 2250-3153.

[2] International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 1 Jan 2013 Page No. 265-303.

[3] IJCSNS International Journal of Computer Science and Net- work Security, VOL.12 No.12, December 2012.

[4] International Journal of Computer Applications (0975 § 8887) Volume 25§ No.11, July 2011.

[5] IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 1, May 2011.

[6] Kandar Shyamalendu, Maiti Arnab, K-N Secret Sharing Visual Cryptography Scheme For Color Image Using Random Number International Journal of Engineering Science and Technology, Vol 3, No. 3, 2011, pp. 1851-1857.

[7] International Journal of Security and Its Applications Vol. 4, No. 2, April, 2010.

[8] Kang InKoo el. at., Color Extended Visual Cryptography using Error Diusion, IEEE 2010.

[9] Journal of Computing, Volume 2, Issue 4, April 2010, ISSN 2151-9617.

[10] Sai Chandana B., Anuradha S., A New Visual Cryptography Scheme for Color Images, International Journal of Engineering Science and Technology, Vol 2 (6), 2010.

[11] M. Naor and A. Shamir, “Visual cryptography”, Advances in Cryptology-Eurocrypt'94, 1995, pp.1-12

[12] Schildt, H. The Complete Reference Java 2, Fifth Ed. TMH, Pp 799-839.

[13] Krishmoorthy R, Prabhu S, Internet & Java Programming, New Age International, pp 23.

[14] John F Koegel Buford, Multimedia Systems, Addison Wesley, 2000.