VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"JnanaSangama", Belagavi-18, Karnataka, India.

A Technical Seminar report on

"VISUAL CRYPTOGRAPHY AND STEGANOGRAPHY"

Seminar report Submitted in partial fulfillment of the requirement for the degree of

Bachelor of Engineering

In

Telecommunication Engineering

By

ARAVINDA V

(1DS16TE024)

8th sem B.E

Under the guidance of

Dr. SMITHA SASI

ASSOCIATE PROFESSOR

Department of Telecommunication Engineering

Accredited by National Board of Accreditation Council (NBA)

DAYANANDA SAGAR COLLEGE OF ENGINEERING

BENGALURU- 560078.

2019-20

DAYANANDA SAGAR COLLEGE OF ENGINEERING

Shavige Malleshwara Hills, Kumaraswamy Layout, Bangalore-560078
(Accredited by NAAC with 'A' Grade, UGC & ISO 9001:2008 Certified)

DEPARTMENT OF TELECOMMUNICATION ENGINEERING

Accredited by National Board of Accreditation Council (NBA)

CERTIFICATE

This is to certify that the Technical seminar report entitled **"Visual Cryptography And Steganography"** is a bonafide work carried out by **ARAVINDA V** (1DS16TE024) of VIII semester, Department of Telecommunication Engineering, DSCE an autonomous institute affiliated to **Visvesvaraya Technological University** in partial fulfillment for the Degree of **Bachelor of Engineering** during the year 2019-20. It is certified that all the suggestion indicated has been incorporated in the report.

Signature of Guide
Dr. SMITHA SASI
Associate Professor
Department of Telecommunication Engineering,
DSCE.

Signature of HOD
Dr. A R ASWATHA
Professor and Head
Department of Telecommunication Engineering,
DSCE.

ACKNOWLEDGEMENT

I wish to express my sincere gratitude to respected **Dr. C.P.S PRAKASH**, Principal, Dayananda Sagar College of Engineering, Bengaluru for providing me an opportunity to present the technical seminar on "**Visual Cryptography And Steganography**".

I am grateful for the constant encouragement and cooperation from my honorable Head of Department, **Dr A.R.ASWATHA**, Telecommunication Engineering Department, Dayananda Sagar College of Engineering, Bengaluru.

My sincere thanks to my guide, **Dr. SMITHA SASI**, Associate Professor of Telecommunication Department in guiding and encouraging me throughout the seminar.

I also thank our seminar coordinator **Mr.VIVEK RAJ K,** Assistant Professor of Telecommunication Department for his support throughout the seminar phase.

ARAVINDA V

(1DS16TE024)

ABSTRACT

Visual cryptography is an algorithm used for encrypting digital media like images, text etc. in which the decryption can be performed by visual mechanical operations rather than using a computer. One of the best-known techniques has been credited to Moni Naor and Adi Shamir, who developed it in 1994. They demonstrated a visual secret sharing 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 and using opaque sheets but illuminating them by multiple sets of identical illumination patterns under the recording of only one single-pixel detector.

In seminar report, a novel visual cryptography scheme with k-n secret sharing is proposed which are then hidden in envelope cover mages using LSB technique for secure data transmission. As the creation of n shares uses random data input, a random number generator algorithm is used for obtain inputs for share generation. This technique needs very less mathematical calculation compare with other existing techniques of visual cryptography on color images.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

The confidentiality of knowledge and data is an important part of the modern system of data communication. Steganography serves as a means of securely transmitting data from one location to another, as digital media can be hacked and altered very easily. Nowadays, steganography is mostly used on computers with digital data being carriers and networks being the high- delivery channels. This is the process of hiding secret information inside the cover media. Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word steganography comes from New Latin steganographia, which combines the Greek words steganós, meaning "covered or concealed", and -graphia meaning "writing".

Cryptography is another process of concealing information. The word cryptography originates from the roots 'crypto' and 'graphy', generally meaning "mystery composing". So as to make data mystery, a figure – a calculation that changes over plain content into ciphertext is utilized, which is mixed up except if a key decodes the figure. The way toward making content mystery is called encryption, and the invert procedure is called decoding. Julius Caesar utilized what's currently called a Caesar figure, to scramble private correspondence. The Caesar figure is one case of a bigger class of strategies called substitution figures. These supplant each letter in a message with something different as indicated by an interpretation. A major downside of essential substitution figures is that letter frequencies are saved. For instance, E is the most widely recognized letter in English, so on the off chance that your figure makes an interpretation of E to a X, at that point X will show up the most regularly in the ciphertext. A talented cryptanalyst can work in reverse from these sorts of insights to make sense of the message.

Another main class of procedures is the Stage figures. Here, a message is taken and filled in to the framework. To scramble the message, the characters are searched in an alternate request, from the bottom left, working upwards, one segment at any

given time. The new letter requesting, known as the stage, is the encoded message. The requesting heading, as well as the lattice measure, fills in as the key. As before, if the figure and key are known, the recipient may invert the procedure to uncover the first message.

Bit plane of an advanced discrete flag, (for example, a picture or sound) is a lot of bits comparing to a given piece position in every one of the double numbers speaking to the flag. For instance, for 16-bit information portrayal there are 16-bit planes: the primary piece plane contains the arrangement of the most critical piece, and the sixteenth contains the least noteworthy piece. It is conceivable to see that the principal bit plane gives the roughest yet the most basic estimate of the estimations of a medium, and the higher the quantity of the bit plane, the less is its commitment to the last stage. In this way, including somewhat plane gives a superior guess. In the event that a bit on the nth piece plane on a m-bit dataset is set to 1, it contributes an estimation of 2(m-n), else it contributes nothing. Along these lines, bit planes can contribute half of the estimation of the past piece plane.

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal. Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned both with concealing the fact that a secret message is being sent and its contents.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the colour of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.

Some of the works and methods of Visual Cryptography and Steganography that are present till date are discussed below-

In Visual Cryptography Scheme for Colour Image Using Random Number with Enveloping by Digital Watermarking, they have taken an extra-planar alpha and represented as a 32 bit for each of the given pixel values and then applying the visual cryptography we are encrypting the image into an „n‟ number of secret shares and placing them into a number of envelopes. And then by simple origin, we are retrieving the shares and also by using a k less than in shares we are reconstructing the original image [1]. In, "Visual cryptography," Advances in Cryptology Eurocrypt‟ by M. Naor and A. Shamir here the authors can decode concealed images without any cryptographic computations. This process is simple and effective. This algorithm was based on the k out of n share creation algorithm. In this process, instead of n shares any of the k shares are sufficient for the decryption of the data [2].

In Multimedia watermarking technology the watermark is hidden inside the cover media in a robust way and the information cannot be extracted without the knowledge of the embedding process. The media that is used in the form of watermark is usually signatures, logo and other stuff that ensures the authentication of the owner. Applications include copyright protection, data monitoring, and data tracking. The authors also explained the scope of watermarking algorithms in different media like the images, videos, audio files text files etc. and finally the drawbacks present in the existing algorithms were summarised [3].

In Comparison of Image Steganography Techniques, Steganography is an area of study where the data has to be transferred from one location to the other. The media that can be used text, video, audio and other digital media. The algorithms discussed in this paper are Least significant bit (LSB), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). The LSB algorithm is spatial based and the DWT and DCT works on the frequency domain. The performance and comparison of these three techniques are evaluated on the basis of the parameters MSE, PSNR, NC, processing time, Capacity& Robustness [4].

CHAPTER 2

VISUAL CRYPTOGRAPHY METHODOLOGY

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption can be done just by sight reading. Visual cryptography, degree associated rising cryptography technology, uses the characteristics of human vision to rewrite encrypted photos. Visual cryptography provides secured digital transmission that is used just for merely the once.

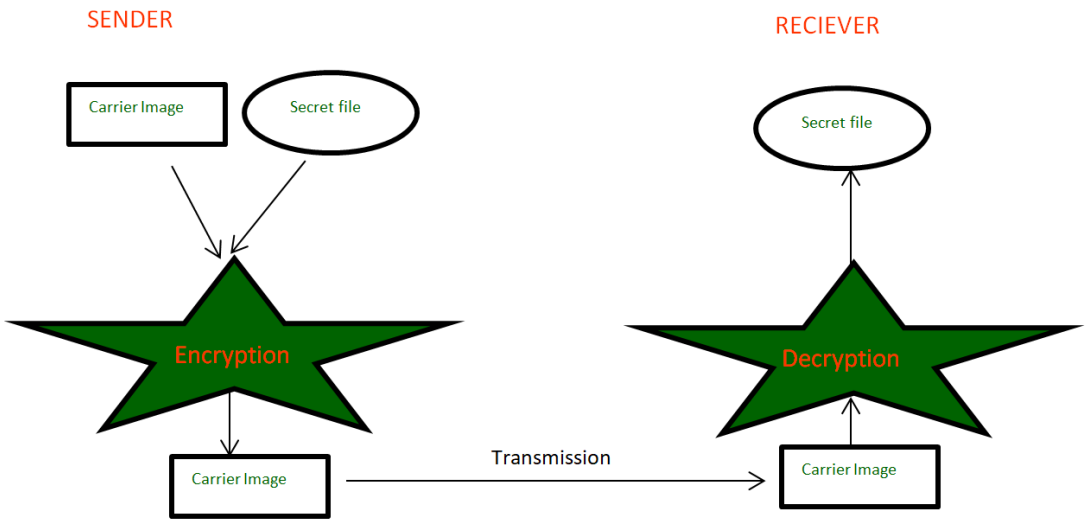


Figure 1. Visual Cryptography General Block Diagram

Numerous guidance like military maps and business identifications are transmitted over the internet. Whereas pattern secret photos, security problems ought to be compelled to be taken into thought as a result of hackers may utilize weak link over the communication network to steal info that they need. To touch upon the protection problems with secret photos, varied image secret sharing schemes are developed. anyone will use it for coding with none science information and any computations.

When the random image contains truly random pixels it can be seen as a one-time pad system and will offer unbreakable encryption. In the overlay animation you can observe the two layers sliding over each other until they are correctly aligned and

the hidden information appears. To understand this, see figure 2, when the layers 1 and 2 are overlapped, we get the required hidden message.

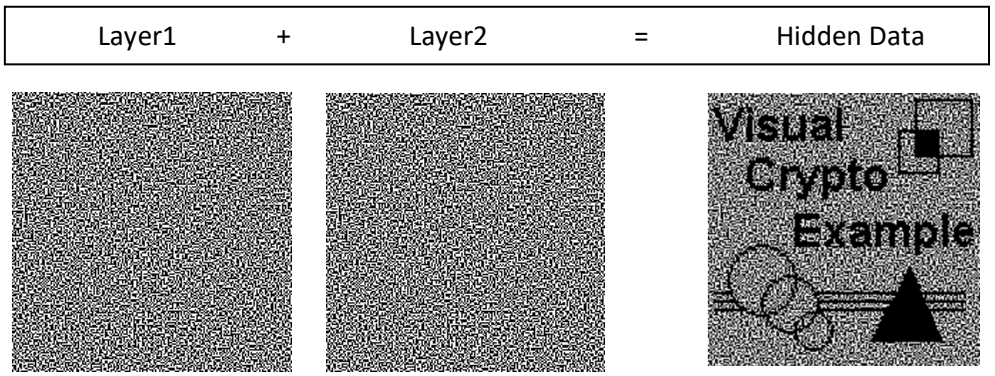


Figure2. Visual cryptography example

Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks. The image in figure2 uses pixels that are divided into four parts.

In the Figure3 we can see that a pixel, divided into four parts, can have six different states. If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlaid pixel will be half black and half white. Such overlaid pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlaid version will be completely black. This is an information pixel.

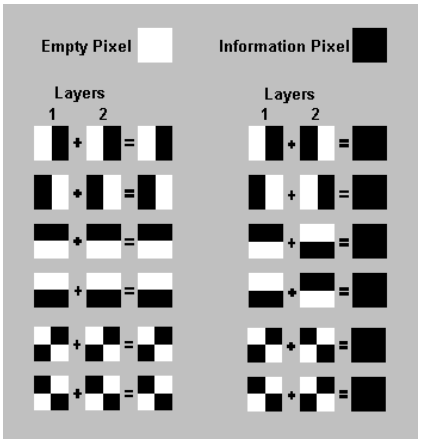


Figure 3. Pixel Combinations

We can now create the two layers. One transparent image, layer 1, has pixels which all have a random state, one of the six possible states. Layer 2 is identical to layer 1, except for the pixels that should be black (contain information) when overlaid. These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlaid, the areas with identical states will look grey, and the areas with opposite states will be black.

The system of pixel can be applied in different ways. In the figure above, each pixel is divided into four blocks. However, you can also use pixels, divided into two rectangle blocks, or even divided circles. Also, it doesn't matter if the pixel is divided horizontally or vertically. There are many different pixel systems, some with better contrast, higher resolution or even with colour pixels.

If the pixel states of layer 1 are truly (crypto secure) random, both empty and information pixels of layer 2 will also have completely random states. One cannot know if a pixel in layer 2 is used to create a grey or black pixel, since we need the state of that pixel in layer 1 (which is random) to know the overlay result. If all requirements for true randomness are fulfilled, Visual Cryptography offers absolute secrecy according to the Information Theory.

If Visual Cryptography is used for secure communications, the sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a message, he creates a layer 2 for a particular distributed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing calculations by hand. The system is unbreakable, as long as both layers don't fall in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information. Visual Cryptography is therefore also a form of secure secret splitting where the two secret shares are required to retrieve the original information.

Like other multimedia components, image is sensed by humans. A pixel is the smallest unit constructing a digital image. Each pixel of a 24-bit digital colour image is divided into four parts, namely Red, Green, Blue (each with 8 bits) and Alpha part represents a degree of transparency.

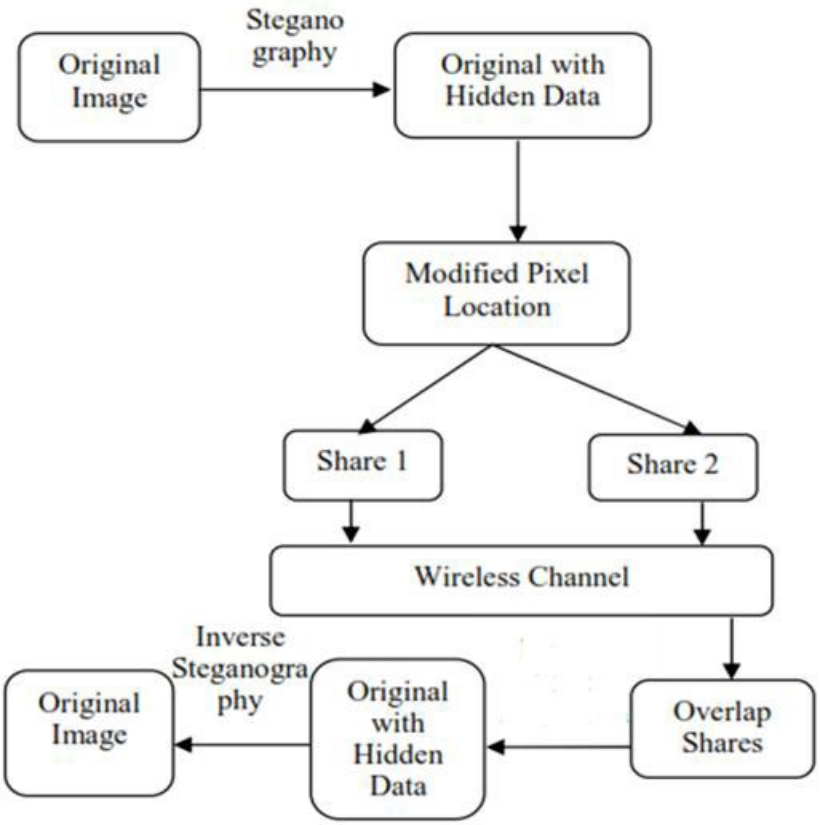


Figure 4. Visual Cryptography Block Diagram

Figure 4. portrays the visual cryptography framework. The human visual framework goes about as an OR work. Two straightforward items stacked together, produce straightforward article, yet changing any of them to non-straightforward, last items will be a non-straightforward article. In k-n mystery sharing visual cryptography conspire a picture is separated into n number of offers with the end goal that the base k number of offers is adequate to reproduce the picture. The division is finished by Random Number generator [5]. This kind of visual cryptography method is unreliable as the reproduction is finished by straightforward OR task. To add greater security to this plan we have proposed a strategy called advanced encompassing. This is only an all-encompassing type of imperceptible computerized watermarking method. Utilizing this procedure, the profit shares delivered by k-n mystery sharing visual cryptography are implanted into the envelope pictures by LSB substitution [6]. The shading change of the envelope pictures isn't detected by the human eye [3]. (More than 16.7 million I. e. 224 distinct hues are created by the RGB shading model. Be that as it may, human eye can segregate just a couple of them.). This system is referred to as undetectable

computerized watermarking as human eye can't distinguish the adjustment in the envelope picture and the envelope (Produced after LSB substitution) picture [8]. In the decoding procedure k number of inserted envelope pictures are taken and LSB are recovered from every one of them pursued by OR task to produce the first picture. The algorithm for the process described in Figure 4 is given below-

2.1 ALGORITHM

Step I: The source image is divided into the planes and a secret image are taken and the steganography technique is applied to these images using bit plane coding algorithm.

Step II: The stego image is then divided into a number of shares using k-n secret sharing visual cryptography scheme. Then all these shares are placed in the envelope images using LSB replacement.

Step III: The shares are retrieved by collecting the LSB's and then the original image is retrieved by combining shares.

Step IV: Then the secret image is retrieved by extracting all the bits from the respective biplane using the bit plane decoding algorithm.

2.2 STEGANOGRAPHY

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. Steganography can be used to conceal almost any type of digital content, including text, image, video or audio content; the data to be hidden can be hidden inside almost any other type of digital content. The content to be concealed through steganography -- called hidden text -- is often encrypted before being incorporated into the innocuous-seeming cover text file or data stream. If not encrypted, the hidden text is commonly processed in some way in order to increase the difficulty of detecting the secret content.

Steganography is practiced by those wishing to convey a secret message or code. While there are many legitimate uses for steganography, malware developers have also been found to use steganography to obscure the transmission of malicious code. Forms of steganography have been used for centuries and include almost any technique for hiding a secret message in an otherwise harmless container. For example, using invisible ink to hide secret messages in otherwise inoffensive messages; hiding documents recorded on microdot -- which can be as small as 1 millimetre in diameter -- on or inside legitimate-seeming correspondence; and even by using multiplayer gaming environments to share information.

The practice of adding a watermark -- a trademark or other identifying data hidden in multimedia or other content files -- is one common use of steganography. Watermarking is a technique often used by online publishers to identify the source of media files that have been found being shared without permission.

According to the given source image either RGB or grayscale image with the given image is divided into number of planes. If it is an RGB image we have 3 planes. A grayscale image is taken as secret image. By taking a bit plane of the secret image, it is coded into the source image and then into any one of the R, G or B plane. Likewise, we are coding them into all the three planes. Then the output image is a stego-image.

2.3 K-N SECRET SHARING VISUAL CRYPTOGRAPHY SCHEME

This scheme divides a secret data S into n number of shares let S1, S2……Sn such that-

i) Knowledge of k or more shares among Si (i n) can reveal the secret information.

ii) Knowledge of less than k shares reveal no information about the secret share.

This technique is called (k, n) secret sharing. The technique is described with an example in the following section. The (k, n) secret sharing comes from the concept that k points are necessary to define a polynomial of degree (k−1). To construct the polynomial, (k−1) coefficients a1, a2…. ak−1 are required. Here a0= S, the secret data. The polynomial f(x) = a0 + a1x + a2x2 + …. +ak−1xk−1 is constructed from the coefficients.

Total n points let i=0…. n is taken and corresponding f(x) are also calculated. From these values n number of pairs (i, f(i)) are constructed. The original coefficients are retrieved by interpolation method from at least k numbers of these pairs [8].

The stego-image is taken as the input to the k-n secret sharing in which n number of shares and then k number of shares are used to re-construct the stego-image. This is done by using a random number. The stego-image is divided into a bit stream of length 24 characters. Create a 3-D matrix of size [an X (w*h) X 24] check for the 1‟s in obtaining bit stream and then replace the same subscript where the 1‟s are obtained with the 1‟s in the matrix created. Thus, a matrix is obtained with n number of shares each share in a row. Reconstruct the pixel values using this particular bit stream of 24 characters in a pixel value so as to get all the shares differently.

2.4 LSB REPLACEMENT

Then the given shares are placed in the envelopes which are 4 times larger than the size of each share. It means that the envelope should be a size of 4 times the width of the share generated. This is done by the process called LSB bit replacement. „n‟ number of envelopes are taken for the „n‟ number of shares and then all the envelope images are converted into a bit stream of 24-bit length each pixel value.

Then the two LSB‟s of the envelope is replaced with the shares bit stream. All the bits are then constructed back into pixel values to construct the image back. Thus, if only the last two LSB’s is changing the human eye can’t make out any difference in the image constructed. So, there will be no change in the envelope image constructed.

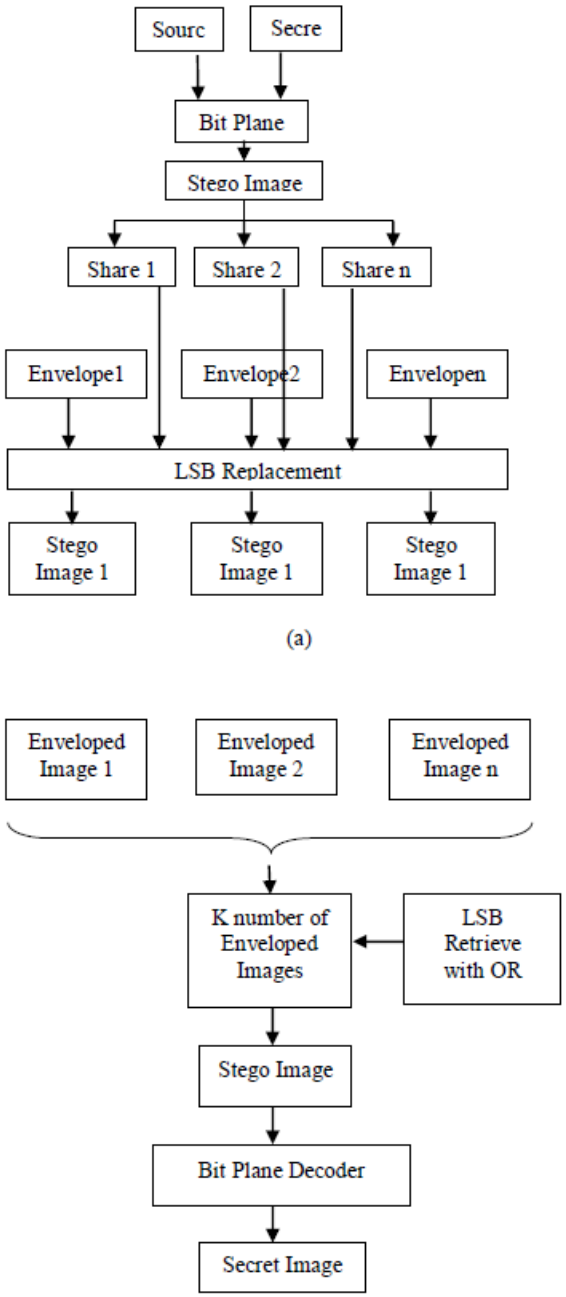


Figure 5. Block Diagram of Overall Process (a) data hiding (b) watermark extraction

2.5 DECRYPTION PROCESS

The decryption process starts with taking the encrypted images which are the envelope images. These envelope image pixel values are converted into a bit stream of length of 24 bits. Then each of the LSB's is retrieved and then shares are reconstructed using the given envelope images. This process is done by LSB retrieving. Then, by taking all the shares the original image is obtained by

combining all the n number of shares using the k-n secret sharing decryption process. This is done by reconstructing all the pixel values from the bit stream obtained from the k-n secret sharing. Then we obtain a stego-image which has the secret image embedded into it.

2.6 INVERSE STEGANOGRAPHY

In the inverse steganography process the input stego-image is taken and using the bit plane decoding process the secret image is retrieved. This is done by using the bit plane number and retrieving all the bits from that particular bit plane and reconstructing the secret image. Thus, the secret image is retrieved from the stego-image.

2.7 EXPERIMENTAL RESULTS

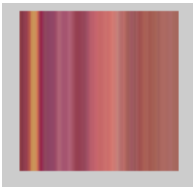
The experimental results for the above proposed algorithm from the paper studied is given below-

Figure 6. Cover Image

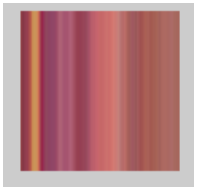
Figure 7. Secret image

Figure 8. Stego Image

Share 1



Share 2



Share 3

Envelope 1

Envelope 2

Envelope 3

Figure 9. Shares and Envelopes used for Transmission

Stego Image 1

Stego Image 2

Stego Image 3

Figure 10. Stego Images

Figure 11. Extracted Secret Image

CHAPTER 3

APPLICATIONS

3.1 APPLICATIONS OF VISUAL CRYPTOGRAPHY

Visual cryptography is a cryptographic technique which allows visual information to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. In this paper, we intend to study the different application areas of Visual Cryptography. Visual Cryptography is a wide area of research used in data hiding, securing images, colour imaging, multimedia and other such fields. Visual Cryptography comes in the field of data hiding used in cybercrime, file formats etc.

Some of the prominent applications include the following-

- **Biometric Security**
- **Secret Communication**
- **Copyright Protection**
- **Document Authentication**
- **Secret data storing**
- **Watermarking**
- **Remote Electronic Voting**
- **Banking Customer identification**

3.2 APPLICATIONS OF STEGANOGRAPHY

Steganography is applicable to the following areas. The area differs in what feature of the steganography is utilized in each system.

- **Confidential communication and secret data storing**

  The "secrecy" of the embedded data is essential in this area.
  Steganography provides us with:
  (A) Potential capability to hide the existence of confidential data

(B) Hardness of detecting the hidden (i.e., embedded) data

(C) Enhancing the secrecy of the encrypted data

One simplest application is to your writing. Attaching a stego file to an e-mail message is another example in this application area. But you and your party must do a "sending-and-receiving" action that could be noticed by a third party. So, e-mailing is not a completely secret communication method.

There is an easy method that has no key-negotiation. We have a model of "Anonymous Covert Mailing System."

- **Protection of data alteration**

We take advantage of the fragility of the embedded data in this application area. We asserted in the Home Page that "the embedded data can rather be fragile than be very robust." Actually, embedded data are fragile in most steganography programs. Especially, Qtech Hide & View program embeds data in an extremely fragile manner. However, this fragility opens a new direction toward an information-alteration protective system such as a "Digital Certificate Document System." The most novel point among others is that "no authentication bureau is needed." If it is implemented, people can send their "digital certificate data" to any place in the world through Internet. No one can forge, alter, nor tamper such certificate data. If forged, altered, or tampered, it is easily detected by the extraction program.

- **Access control system for digital content distribution**

In this area embedded data is "hidden", but is "explained" to publicize the content. Today, digital contents are getting more and more commonly distributed over Internet than before. For example, music companies release new albums on their Webpage in a free or charged manner. However, in this case, all the contents are equally distributed to the people who can make access to the page. So, an ordinary Web distribution scheme is not suited for a "case-by-case" and "selective" distribution. Of course, it

is always possible to attach digital contents to e-mail messages and send them to the customers. But it will take a lot of cost in time and labour.

If you have some valuable content, which you think it is distributable if someone really needs it, and if it is possible to upload that content on Internet in some covert manner. And if you can issue a special "access key" to extract the content selectively, you will be very happy about it. A steganographic scheme can help realize this type of system.

- **Media Database systems**

  In this application area of steganography secrecy is not important, but unifying two types of data into one is the most important.

  Media data (photo picture, movie, music, etc.) have some association with other information. A photo picture, for instance, may have the following.

  (1) The title of the picture and some physical object information
  (2) The date and the time when the picture was taken
  (3) The camera and the photographer's information

  Formerly, these are annotated beside each picture in the album.

  Recently, almost all cameras are digitalized. They are cheap in price, easy to use, quick to shoot. They eventually made people feel reluctant to work on annotating each picture. Now, most home PC's are stuck with the huge amount of photo files. In this situation it is very hard to find a specific shot in the piles of pictures. A "photo album software" may help a little. You can sort the pictures and put a couple of annotation words to each photo. When you want to find a specific picture, you can make a search by keywords for the target picture. However, the annotation data in such software are not unified with the target pictures. Each annotation only has a link to the picture. Therefore, when you transfer the pictures to a different album software, all the annotation data are lost.

  This problem is technically referred to as "Metadata (e.g., annotation data) in a media database system (a photo album software) are separated from

the media data (photo data) in the database managing system (DBMS)." This is a big problem.

Steganography can solve this problem because a steganography program unifies two types of data into one by way of embedding operation. So, metadata can easily be transferred from one system to another without hitch. Specifically, you can embed all your good/bad memory (of your sight-seeing trip) in each snap shot of the digital photo. You can either send the embedded picture to your friend to extract your memory on his/her PC, or you may keep it silent in your own PC to enjoy extracting the memory ten years after.

CHAPTER 4

CONCLUSION

Visual cryptography is an algorithm used for encrypting digital media like images, text etc. in which the decryption can be performed by visual mechanical operations rather than using a computer. Visual Cryptography and steganography, both concepts are studied and understood in detail. In this report, a novel visual cryptography scheme with k-n secret sharing is presented which are then hidden in envelope cover mages using LSB technique for secure data transmission. This adds security to visual cryptography technique from illicit attack as it befools the hackers‟ eye.

Steganography is not intended to replace cryptography but supplement it. Hiding a message with steganography methods reduces the chance of a message being detected. However, if that message is also encrypted, if discovered, it must also be cracked. There are an infinite number of steganography applications. Steganography does not only pertain to digital images but also to other media. If an encrypted message is intercepted, the interceptor knows the text is an encrypted message. With steganography, the interceptor may not know the object contains a message.

The division of a picture into n number of offers is finished by utilizing an irregular number generator, which is another method not accessible till date. This method needs less scientific count contrast and other existing procedures of visual cryptography on shading pictures. This method just checks „1‟ at the bit position and gap that „1‟ into (nk+1) shares utilizing irregular numbers. An examination is made to the proposed plan with some different plans to demonstrate the curiosity of the plan.

CHAPTER 5

REFERENCES

[1] Visual Cryptography Scheme for Colour Image Using Random Number with Enveloping by Digital Watermarking by Shyamalendu Kandar, Arnab Maiti, Bibhas Chandra Dhara, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 1, May 2011

[2] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology-Eurocrypt"94, 1995, pp. 1–12.

[3] Hartung, F., Cutter M., "Multimedia Watermarking Techniques", IEEE, 1999.

[4] Stuti Goel, Arun Rana, Manpreet Kaur; "Comparison of Image Steganography Techniques", Mathematics, Semantic Scholor,2013.

[5] 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.

[6] Naskar P., Chaudhuri A, Chaudhuri Atal, Image Secret Sharing using a Novel Secret Sharing Technique with Steganography, IEEE CASCOM, Jadavpur University, 2010, pp 6265.

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

[8] Shyamalendu Kandar, Bibhas Chandra Dhara; "k-n Secret Sharing Visual Cryptography Scheme on Color Image using Random Sequence"; International Journal of Computer Applications (0975 – 8887) Volume 25– No.11, July 2011.

ADVANCED ROBUST DATA HIDING USING VISUAL CRYPTOGRAPHY

LEELAVATHI RUDRAKSHA
Electronics and Communications Engineering,
Vasavi college of engineering,
Hyderabad, India
leelavathirudraksha@gmail.com

GIRI PRASAD M.N.
Electronics and Communications Engineering,
JNTU College of Engineering,
Anantapuramu, India
mahendragiri1960@gmail.com

***Abstract*—Visual cryptography is an algorithm used for encrypting digital media like images, text etc in which the decryption can be performed by visual mechanical operations rather than using a computer. In this paper, a novel visual cryptography scheme with k-n secret sharing is proposed which are then hidden in envelope cover mages using LSB technique for secure data transmission. As the creation of n shares uses random data input, a random number generator algorithm is used for obtain inputs for share generation. This technique needs very less mathematical calculation compare with other existing techniques of visual cryptography on color images.**

Keywords— data hiding, encryption, decryption, LSB replacement, DCT, DWT, visual cryptography

I. INTRODUCTION

Information security is an integral part of the modern data transmission system. Steganography serves as s means of securely transmitting the data from one place to another as the digital media can be hacked and altered very easily. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. This is the process of hiding secret information inside cover media. Another process of concealing the information is cryptography.

The word cryptography originates from the roots 'crypto' and 'graphy', generally meaning "mystery composing". So as to make data mystery, a figure – a calculation that changes over plain content into ciphertext is utilized, which is mixed up except if a key decodes the figure. The way toward making content mystery is called encryption, and the invert procedure is called decoding. Figures have been utilized well before PCs appeared. Julius Caesar utilized what's currently called a Caesar figure, to scramble private correspondence. He would move the letters in a message forward by three spots. Along these lines, A progressed toward becoming D, and "brutus" turned into this: "euxwxv". To interpret the message, beneficiaries needed to know both the calculation and the number to move by, which went about as the key. The Caesar figure is one case of a bigger class of strategies called substitution figures. These supplant each letter in a message with something different as indicated by an interpretation.

A major downside of essential substitution figures is that letter frequencies are saved. For instance, E is the most widely recognized letter in English, so on the off chance that your figure makes an interpretation of E to a X, at that point X will show up the most regularly in the ciphertext. A talented cryptanalyst can work in reverse from these sorts of insights to make sense of the message.

Another key class of procedures are stage figures. Here, a message is taken and is filled into a framework. To scramble the message, the characters are perused out in an alternate request, from the base left, working upwards, one segment at any given moment. The new letter requesting, what's known as a stage, is the encoded message. The requesting heading, just as the lattice measure, fills in as the key. Like previously, if the figure and key are known, a beneficiary can invert the procedure to uncover the first message. By the 1900s, cryptography was motorized as encryption machines.

Bit plane of an advanced discrete flag, (for example, a picture or sound) is a lot of bits comparing to a given piece position in every one of the double numbers speaking to the flag. For instance, for 16-bit information portrayal there are 16 bit planes: the primary piece plane contains the arrangement of the most critical piece, and the sixteenth contains the least noteworthy piece. It is conceivable to see that the principal bit plane gives the roughest yet the most basic estimate of the estimations of a medium, and the higher the quantity of the bit plane, the less is its commitment to the last stage. In this way, including somewhat plane gives a superior guess. In the event that a bit on the nth piece plane on a m-bit dataset is set to 1, it contributes an estimation of 2(m-n), else it contributes nothing. Along these lines, bit planes can contribute half of the estimation of the past piece plane.

In this paper, section I contains a brief about the need for information security and the algorithms available. Section II presents a description of the algorithms used by authors working in this domain. Section III describes the visual cryptography algorithm and the detailed explanation of the proposed technique. The experimental results are illustrated in section IV which is followed by conclusion.

II. LITERATURE

In Visual Cryptography Scheme for Color Image Using Random Number with Enveloping by Digital Watermarking by Shyamalendu Kandar, Arnab Maiti, Bibhas Chandra Dhara here the authors have taken an extra-planar alpha and represented as a 32 bit for each of the given pixel values and then applying the visual cryptography we are encrypting the image into an „n‟ number of secret shares and placing them into a number of envelopes. And then by simple origin, we are retrieving the shares and also by using a k less than in shares we are reconstructing the original image. In, “Visual cryptography,” Advances in CryptologyEurocrypt‟ by M. Naor and A. Shamir here the authors can decode concealed images without any cryptographic computations. This process is simple and effective. This algorithm was based on the k out of n share creation algorthm. In this process,

978-1-5386-8158-9/19/$31.00©2019IEEE

instaed of n shares any of the k shares are sufficient for the decryption of the data.

In Multimedia watermarking technology by Hartung F. Cutter M.A the watermark is hidden iside the cover media ina robust way and the information cannot be extracted without the knowledge of the embedding process.The media that is used in the form of watermark is usually signatures, logo and other stuff that ensures the authentication of the owner. Applications include copyright protection, data monitoring, and data tracking. The authors also expplained the scope of watermarking algorithms in different media like the images, videos, audio files text files etc. and finally the drwawbacks present in the exisitng algorithms were summarised.

In Comparison of Image Steganography Techniques byStuti Goel, Arun Rana, Manpreet Kaur Steganography is an area of study where the data has to be tranfered from one location to the other. The media that can be used text, video, audio and other digital media. The algorithms discussed in this paper are Least significant bit (LSB), Descrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT).The LSB algorithm is spatial based and the DWT and DCT works on the frequency domain. The performance and comparison of these three techniques are evaluated on the basis of the parameters MSE, PSNR, NC, processing time, Capacity& Robustness.

III. VISUAL CRYPTOGRAPHY

Like other multimedia components, image is sensed by humans. A pixel is the smallest unit constructing a digital image. Each pixel of a 24 bit digital color image is divided into four parts, namely Red, Green, Blue (each with 8 bits) and Alpha part represents a degree of transparency.

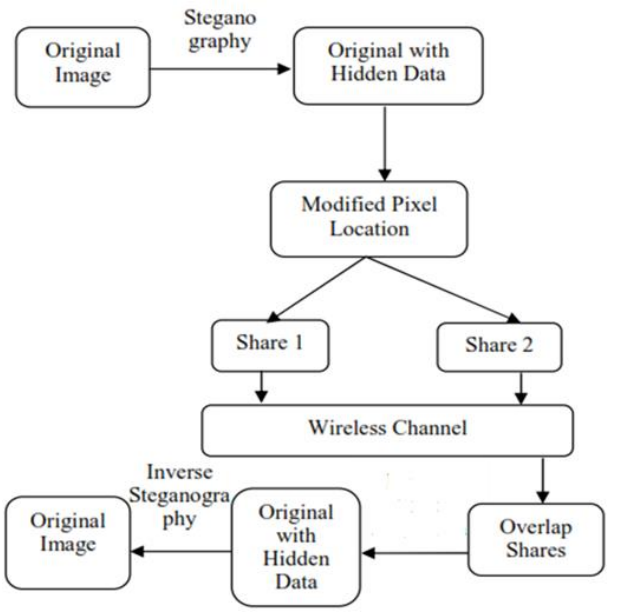


Figure 1. Visual Cryptography Block Diagram

Figure 1 portrays the visual cryptography framework. The human visual framework goes about as an OR work. Two straightforward items stacked together, produce straightforward article, yet changing any of them to non-straightforward, last items will be a non-straightforward article. In k-n mystery sharing visual cryptography conspire a picture is separated into n number of offers with the end goal that the base k number of offers is adequate to reproduce the picture. The division is finished by Random Number generator [4]. This kind of visual cryptography method is unreliable as the reproduction is finished by straightforward OR task. To add greater security to this plan we have proposed a strategy called advanced encompassing. This is only an all-encompassing type of imperceptible computerized watermarking method. Utilizing this procedure, the profit shares delivered by k-n mystery sharing visual cryptography are implanted into the envelope pictures by LSB substitution [5]. The shading change of the envelope pictures isn't detected by the human eye [6]. (More than 16.7 million I. e. 224 distinct hues are created by the RGB shading model. Be that as it may, human eye can segregate just a couple of them.). This system is referred to as undetectable computerized watermarking as human eye can't distinguish the adjustment in the envelope picture and the envelope (Produced after LSB substitution) picture [7]. In the decoding procedure k number of inserted envelope pictures are taken and LSB are recovered from every one of them pursued by OR task to produce the first picture.

A. Overall process: Algorithm

Step I: The source image is divided into the planes and a secret image are taken and the steganography technique is applied to these images using bit plane coding algorithm.

Step II: The stego image is then divided into a number of shares using k-n secret sharing visual cryptography scheme. Then all these shares are placed in the envelope images using LSB replacement.

Step III: The shares are retrieved by collecting the LSB‟s and then the original image is retrieved by combining shares.

Step IV: Then the secret image is retrieved by extracting all the bits from the respective biplane using the bit plane decoding algorithm.

Figure 1 describes the steps involved in the algorithm.

B. Steganography:

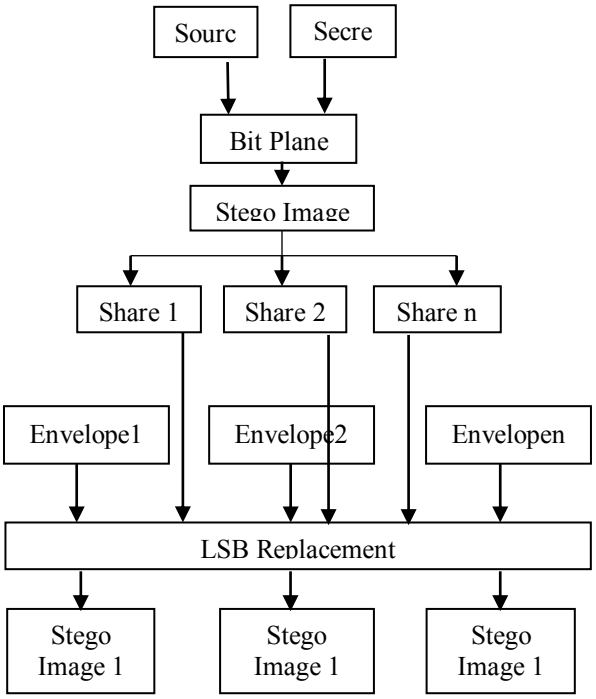
According to the given source image either RGB or grayscaleimage with the given image is divided into number of planes. If it is an RGB image we have 3 planes. A grayscale image is taken as secret image. By taking a bit plane of the secret image, it is coded into the source image and then into any one of the R, G or B plane. Likewise, we are coding them into all the three planes. Then the output image is a stego-image.

C. k-n secret sharing visual cryptography scheme

The stego-image is taken as the input to the k-n secret sharing in which n number of shares and then k number of shares are used to re-construct the stego-image. This is done by using a random number. The stego-image is divided into a bit stream of length 24 characters. Create a 3-D matrix of size [an X (w*h) X 24] check for the 1‟s in obtaining bit stream and then replace the same subscript where the 1‟s are obtained with the 1‟s in the matrix created. Thus a matrix is obtained with n number of shares each share in a row. Reconstruct the pixel values using this particular bit stream of 24 characters in a pixel value so as to get all the shares differently.

D. LSB replacement

Then the given shares are placed in the envelopes which are 4 times larger than the size of the each share. It means that the envelope should be a size of 4 times the width of the share generated. This is done by the process called LSB bit replacement. „n" number of envelopes are taken for the „n" number of shares and then all the envelope images are converted into a bit stream of 24 bit length each pixel value.



(a)

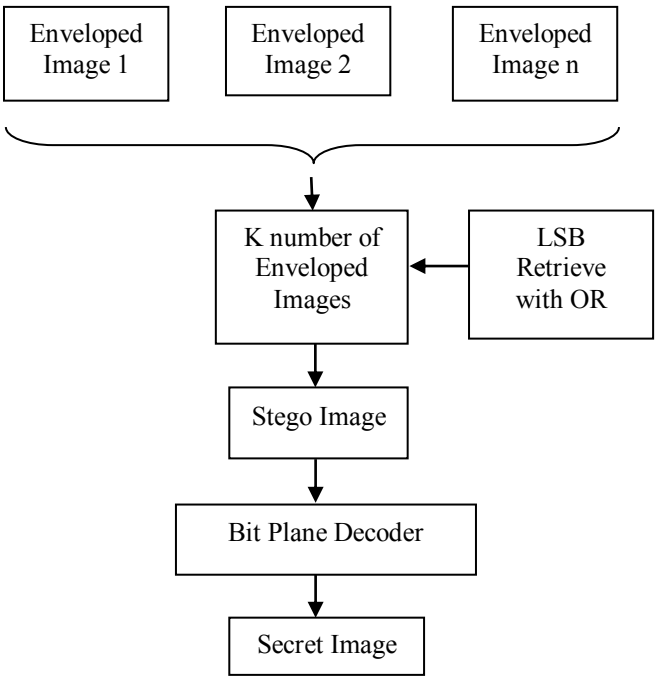


Fig 2. Block Diagram of Overall Process (a) data hiding (b) watermark extraction

Then the two LSB"s of the envelope is replaced with the shares bit stream. All the bits are then constructed back into pixel values to construct the image back. Thus, if only the last two LSB"s are changing the human eye can"t make out any difference in the image constructed. So there will be no change in the envelope image constructed.

E. Decryption process

The decryption process starts with taking the encrypted images which are the envelope images. These envelope image pixel values are converted into a bit stream of length of 24 bits. Then each of the LSB"s are retrieved and then shares are reconstructed using the given envelope images. This process is done by LSB retrieving. Then, by taking all the shares the original image is obtained by combining all the n number of shares using the k-n secret sharing decryption process. This is done by reconstructing all the pixel values from the bit stream obtained from the k-n secret sharing. Then we obtain a stego-image which has the secret image embedded into it.

F. Inverse Steganography

In the inverse steganography process the input stego-image is taken and using the bit plane decoding process the secret image is retrieved. This is done by using the bit plane number and retrieving all the bits from that particular bit plane and reconstructing the secret image. Thus the secret image is retrieved from the stego-image.

IV. Experimental Results

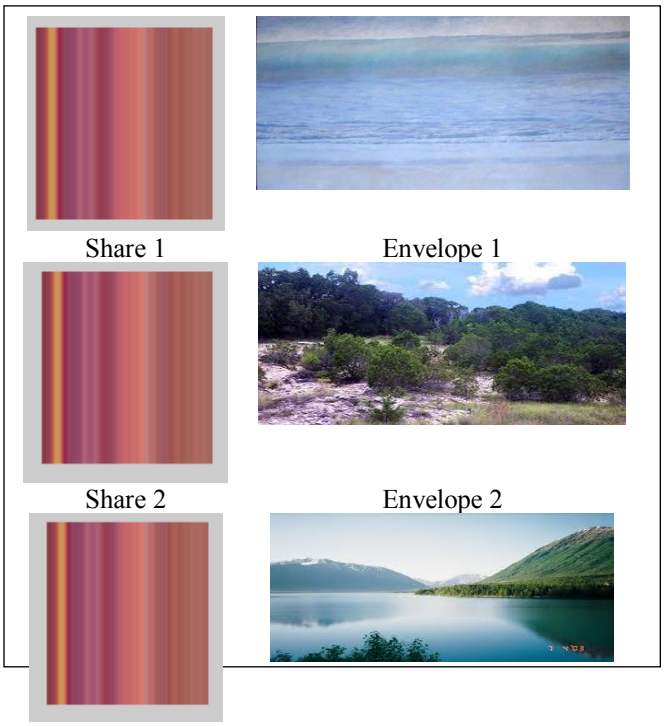
The figures 3 and 4 present the cover image and secret image respectively.

Fig 3. Cover Image

Fig 4. Secret Image

Fig 5. Stego Image

Figure 5 shows the output stego image



Stego Image 1

Stego Image 2

Stego Image 3

Fig 7. Stego Images

Fig 8. Extracted Secret Image

CONCLUSION

Visual cryptography is an algorithm used for encrypting digital media like images, text etc in which the decryption can be performed by visual mechanical operations rather than using a computer. In this paper, a novel visual cryptography scheme with k-n secret sharing is proposed which are then hidden in envelope cover mages using LSB technique for secure data transmission. This adds security to visual cryptography technique from illicit attack as it befools the hackers‟ eye. The division of a picture into n number of offers is finished by utilizing an irregular number generator, which is another method not accessible till date. This method needs less scientific count contrast and other existing procedures of visual cryptography on shading pictures [10] [11] [12] [13]. This method just checks „1‟ at the bit position and gap that „1‟ into (nk+1) shares utilizing irregular numbers. An examination is made to the proposed plan with some different plans to demonstrate the curiosity of the plan.

REFERENCES

The template will number citations consecutively within brackets [1]. The sentence punctuation follows the brackets [2]. Simply refer to the reference number, as in [3] —do not use “Ref. [3]” or “reference [3]” except at the beginning of a sentence: “Reference [3] was the first...”

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the abstract or reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors’ names; do not use “et al.”. Papers that have not been published, even if they have been submitted for publication, should be cited as “unpublished” [4]. Papers that have been accepted for publication should be cited as “in press” [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

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

[2] P. Ranjan, “Principles of Multimedia”, Tata McGraw Hill, 2006.

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

[4] 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.

[5] Naskar P., Chaudhuri A, Chaudhuri Atal, Image Secret Sharing using a Novel Secret Sharing Technique withSteganography, IEEE CASCOM, Jadavpur University, 2010, pp 6265.

[6] Hartung, F., Cutter M., "Multimedia Watermarking Techniques", IEEE, 1999.

[7] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung. Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications. IEEE Journal on Selected Areas in Communications, Vol16, No.4 May 1998, pp. 573–586.

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

[9] Krishmoorthy R, Prabhu S, Internet & Java Programming, New Age International, pp 234.

[10] F. Liu1, C.K. Wu1, X.J. Lin, color visual cryptography schemes, IET Information Security, July 2008.

[11] Kang InKoo el. at., Color Extended Visual Cryptographyusing Error Diffusion, IEEE 2010.

[12] SaiChandana B., Anuradha S., A New Visual CryptographyScheme for Color Images, International Journal of Engineering Science and Technology, Vol 2 (6), 2010.

[13] Li Bai, A Reliable (k,n) Image Secret Sharing Scheme by,IEEE,2006. G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*,