International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-5 Issue-3, February 2016

Encryption and Decryption Process of a Secret Natural Colour Image Based on K out of N VSS Scheme

Debabrata Bhattacharya, Harinandan Tunga

Abstract: ***The Visual Secret Sharing (VSS) scheme is a cryptographic tool used to encode a secret image into several shares, each of which separately does not reveal any information of the secret image. Visual Cryptography (VC) schemes hide the secret image into two or more images which are called 'shares'. The secret image can be recovered simply by stacking the shares together without any complex computation involved. The shares are very safe because separately they reveal nothing about the secret image. In this paper, a generalized version of Visual Cryptography is mentioned. Here an image (secret image) can be hidden in 'n' numbers of cover images. This generalized version helps the user to attain the desired level of encryption. Also after successful transmission the secret image can be re-discovered using a simple decryption algorithm. The aim of our paper is that a sender sends 'n' number of colored images with a hidden secret image in it by encryption and the receiver recovers the secret image from it by decryption. The proposed approach uses meaningful shares (cover images) to hide the colored secret image and the recovery process is lossless. In this paper, we propose a proportionate algorithm which successfully encrypts a secret image into any number of cover images as chosen by the user. Here the amount of original image share depends upon the pixel values of the cover images. Also a critical value on the number of images is determined which helps in optimizing our aim with the complexity.***

Keywords: Visual Cryptography (VC), Secret Image, Hidden Secret Image, Proportionate Algorithm, Human Vision System (HVS)

I. INTRODUCTION

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc) to be encrypted in such a way that the decryption can be performed by the human visual system without the aid of computers. The possibility of using human visual intelligence as part of a symmetrical cipher algorithm was discussed. Independently, the notion of visual k out of n secret sharing schemes is introduced. The idea is that an image (e.g. picture or text) is transformed into 'n' transparencies (shares), in such a way that if one puts any k-tuple of transparencies on top of each other, the original image is again visible, while with any (k-1)-tuple of transparencies no information about the original image is released (in the sense that any possibility is equally likely). Actually,

Manuscript published on 28 February 2016.
* Correspondence Author (s)
Debabrata Bhattacharya, Department of Applied Electronics & Instrumentation Engineering, Regional Computer Centre Institute of Information Technology, Kolkata (West Bengal). India.
Harinandan Tunga, Department of Computer Science and Engineering, Regional Computer Centre Institute of Information Technology, Kolkata (West Bengal). India.

The concept of a visual k out of n secret sharing scheme constitutes a visual symmetrical cipher earlier described. The technique explained divides any pixel of the original image into b sub-pixels. On each transparency some sub-pixels of any pixel are white while the others are black. When held to the light, white sub-pixels let light go through and black sub-pixels stop it. So when several transparencies on top of each other are held to the light, one sees the "OR" result of the transparencies, i.e. a sub-pixel is seen as white if all underlying sub-pixels are white, otherwise it is seen as black. A pixel (the total of the b sub-pixels) will be observed as white if sufficiently many sub-pixels (at least h) are white, while it will be observed as black if not too many of them (at most l) are white. Here h > l is some non-negative integer. In the mathematical model of this technique, white (sub) pixels are represented with 0 ("they form no obstruction to light") and black (sub) pixels are represented with 1 ("they stop light"). To give a formal definition, let z(v) denote the number of zero coordinates of a vector v (note that z(v)+w(v) = b, where w(v) denotes the Hamming weight of v). From above we now quote, with some notational changes, the following definition of a k out of n secret sharing scheme, or k out of n scheme for short.

The accelerating integration of computer and communication technology, has established Internet worldwide, and multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps and commercial identifications have been converted into multimedia data, stored, and processed for transmission and distribution. While using secret images, security issues should be taken into consideration.

The traditional cryptography, a process of encryption and decryption, is time consuming and requires massive computations. To deal with the security problems of secret images, various image secret sharing schemes have been developed. Visual cryptography scheme eliminates complex computation problem in decryption process thus enabling the transfer of secret images in a more convenient, easy and secure way. In a VCS (Visual Cryptography Scheme) or VSSS (Visual Secret Sharing Scheme) (Shamir [1] 1979), there is a secret image which is encrypted into some share images. The secret image is called the Original Secret Image for clarity, and the share images are called the Encrypted Images (and are called the Transparencies if they are printed out). When a qualified set of share images (Transparencies) are stacked together properly, it gives a visual image which is almost the same as the original secret image; we call this the Recovered Secret Image.

As network technology has been greatly advanced, much information is transmitted via the Internet conveniently and rapidly. At the same time, the security issue is a crucial problem in the transmission process. For example, the information may be intercepted from/during transmission process. Thus process must be developed wherein it will be able to encrypt any image in any standard format, so that the encrypted image when perceived by the naked eye or intercepted by any person with malicious intentions during the time of transmission of the image is unable to be deciphered.

The modern field of Cryptography can be divided into several areas -Symmetric key cryptography refers to the encryption methods in which both the sender and receiver share the same key. A single key is used for both encryption and decryption. There are two different types of keys involved in Public key cryptography: public key and private key. The sender uses the public key of the receiver to encrypt the message and the receiver on the other end uses the private key to decrypt the message.

Visual Cryptography was pioneered by Moni Naor and Adi Shamir in 1994 [2]. They demonstrated a visual secret sharing scheme, where an image was broken into n shares so that only someone with all the n shares can decrypt the image, while any (n-1) shares revealed no information about the original image. The (k, n) visual cryptography schemes (VCS) were introduced by Naor and Shamir in 1994, which is a technique allowing a dealer to encode a secret image into n shares. The secret image is visible if and only if any k shares (k< n) are stacked together, whereas any set of less than k shares cannot gain any information about the secret image. In (k ,n) basic model any k shares will decode the secret image which reduces security level. To overcome this issue the basic model is extended to General Access Structure, where an Access Structure is a specification of all qualified and forbidden subsets of n shares. Any subset of k or more qualified shares can decrypt the secret image but no information can be obtained by stacking lesser number of qualified shares or by stacking disqualified shares. The size of the shares and the implementation complexity in these schemes depends on the number of colors appearing in the secret image. In other words, when the secret image contains a large number of colors, these schemes will become impractical. This scheme provides a more efficient way to hide a gray image (256-colors) in different shares. Naor and Shamir [7] describe the visual secret sharing problem in which the secret image can be viewed as nothing more than a collection of black and white pixels. Each pixel in the original image is divided into a certain number of sub-pixels (m) in each of the n shares. Each share is comprised of collections of m black and white sub-pixels where each collection represents a particular original pixel. When the shares are stacked together in order to align the sub-pixels, the secret image can be recovered.

The important parameters of this scheme are:

• **Pixel expansion** m, which refers to the number of pixels in a share used to encrypt a pixel of the secret image. This implies loss of resolution in the reconstructed image.

• **Contrast** 'α', which is the relative difference between black and white pixels in the reconstructed image. This implies the quality of the reconstructed image. Generally, smaller the value of m will reduce the loss in resolution and greater the value of 'α' will increase the quality of the reconstructed image. As mentioned above if m is decreased the quality of the reconstructed image will be increased but security will be a problem.

So research is focused on two paths

• To have good quality

• To increase security with minimum pixel

Extended Visual Cryptography is a type of cryptography which encodes a number of images in the way that when the images on transparencies are stacked together, the hidden message appears without a trace of original images. The decryption is done directly by the human visual system with no special cryptographic calculations. Generally, visual cryptography suffers from the deterioration of the image quality.

Naor and Shamir [2] applied the above idea on black and white images only. Few years later, Verheul and Tilborg [6], developed a scheme that can be applied on colored images. The inconvenience with these new schemes is that they use meaningless shares to hide the secret and the quality of the recovered image is bad. More advanced schemes based on visual cryptography were introduced where a colored image is hidden into multiple meaningful cover images. Chang, Tsai and Chen [7] proposed a new secret color image sharing scheme, based on the modified visual cryptography. In that scheme, through a predefined Color Index Table (CIT) and a few computations they can decode the secret image precisely. Using the concept of modified visual cryptography, the recovered secret image has the same resolution as the original secret image in their scheme. However, the number of sub-pixels in their scheme is also in proportion to the number of colors appearing in the secret image; i.e. the more colors the secret image has, the larger the shares will become. Another disadvantage is that additional space is needed to store the colors. Chang and Yu [8] introduced a new secret color image sharing scheme based on modified visual cryptography. By means of defining a modified stacking operation, this scheme can hide a gray image (256-colors) among n shares easily and has the ability to recover the hidden image clearly. This scheme does not need any predefined Color Index Table (CIT), and the sizes of shares are the same and fixed. Furthermore, the share size is independent of the number of colors appearing in the secret image. Moreover, the pixel expansion in this scheme is only 9, which is the least among those in the previously proposed methods. This technique achieves a lossless recovery of the secret image but the generated shares (camouflage images) contain excessive noise. This paper introduces an improved scheme based on Chang's technique [8] in order to enhance the quality of the cover images while achieving lossless recovery and without increasing the computational complexity of the algorithm. Encryption is the process of transforming information using above algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The result of the process is encrypted information. As for the encryption process, the information contained in the secret color image is distributed to the other two images called the resulted shares. Resulted shares are now stacked together. The decryption is done directly by the human user's vision. The secret image is revealed by properly stacking the two resulted shares.

II. RELATED WORKS

In literature survey we studied the basic definitions and start from those research papers that are the base of these technologies, then review those papers that are currently available in this technology. Visual cryptography is a popular solution for image encryption. Using secret sharing concepts, the encryption procedure encrypts a secret image into the shares which are noise-like secure images which can be transmitted or distributed over an untrusted communication channel. Using the properties of the HVS to force the recognition of a secret message from overlapping shares, the secret image is decrypted without additional computations and any knowledge of cryptography.

2.1 Basic Concept of 2-out-of-2 VC Scheme

Fig. 2.1 below shows Visual Cryptography scheme where 2 shares are generated from the original secret image and by stacking together the secret is revealed. This is the basic technique, however if we create more than 2 shares and some or all of them stacked for getting the real secret, it is called Visual Secret Sharing(VSS). Following figure shows the basic ideas behind this scheme.

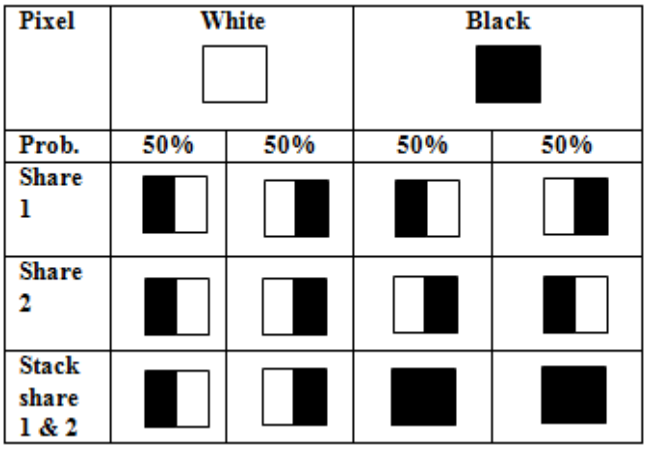

Figure 2.1: Basic concept of 2-out-of-2 VC Scheme

In this concept one white or black pixel will divide into two sub-pixels. One way combination of the pixel divisions is shown in above figure. It is mentioned that the shares 1 and 2 are stacked together and we get the result in the form of complete black or gray pixel (it's partially white and black but visualized as gray). Because of this when we stacked the shares the white in original secret image become gray in the stacked result.

2.1.1 Representation of these shares in Matrix form

These shares can be represented as matrix of S_{ij}; it is a Boolean matrix with shows 1 for black and 0 for white in sub pixels. i.e.

S = [S_{ij}] where

i = a row for each share,

j = a column for each share,

S_{ij}=1 <=> the jth sub pixel of the ith share is dark.

Hence one set of matrices for "0" means white (i.e. for each gray-level in secret image) and one for "1" means black. Normally each set is the column permutations of base matrix; for each pixel, choose a random matrix in the corresponding set (Normally with equal probabilities). The Matrix for the shares in Fig. 2.1 is shown below.

$$S_0 = \left\{ \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

$$S_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

2.1.2 Properties of Sharing Matrices

The major work done in this field is in the direction of *pixel expansion* and *contrast*. As we mentioned above that in the resultant the white color is shown as gray and because we divide the white and black pixels from the original secret image the resultant is double in size with respect to original. For sharing matrix the *contrast* is the sum of the sum of rows since shares in a *decrypting group* should be bigger for darker pixels and for *secrecy* sums of rows in any *non-decrypting group* should have same probability distribution for the number of 1's in S_0 and in S_1.

2.2 (k, n) Secret Sharing Scheme

Naor-Shamir **[2]**, 1994 shows (k, n) secret sharing in their paper. They explained as "an N-bits secret shared among n participants, using m sub pixels per secret bit (n strings of mN), so that any k can decrypt the secret":

Contrast: There are d<m and 0<α<1:
If pixel=1 at least d of the corresponding m sub pixels are dark ("1").
If pixel =0 no more than (d-αm) of the m sub pixels are dark

Security: Any subset of less than k shares does not provide any information about the secret x.
All shares code "0" and "1" with the same number of dark sub pixels in average.

2.2.1 Generalization of (k, n) secret sharing scheme

Naor-Shamir **[2]** generalized their results by using the following theorem/lemma.

Lemma: There is a *(k, k)* scheme with $m=2^{k-1}$, $\alpha=2^{1-k}$ and $r=(2^{k-1}!)$.

We can construct a (5, 5) sharing, with 16 subpixels per secret pixel and 1 pixel contrast, using the permutations of 16 sharing matrices.

Theorem: In any *(k, k)* scheme, $m \geq 2^{k-1}$ and $\alpha \leq 2^{1-k}$.

Theorem: For any *n* and *k*, there is a *(k, n)* visual secret sharing scheme with $m=\log n\, 2^{O(k \log k)}$, $\alpha=2^{-\Omega(k)}$.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

2.2.2 Extensions: General Access Structure

Let P = {1,2,....n} be a set of elements called participants, and let 2^p denote the set of all subsets of P. Let $\Lambda_{Qual} \subseteq 2^p$ and $\Lambda_{Forb} \subseteq 2^p$ and $\Lambda_{Qual} \cap \Lambda_{Forb} = \emptyset$, where

Λ_{Qual} = Qualified set

Λ_{Forb}= Forbidden set

And the pair (Λ_{Qual} , Λ_{Forb}) is called the General Access Structure of scheme.

where Λ_0 defines all minimal qualified set.

$\Lambda_0 = \{A \in \Lambda_{Qual} : A' \notin \Lambda_{Qual}$ for all $A' \subset A\}$

Through this scheme: let us define arbitrary sets Λ_{Qual} and Λ_{Forb} as subsets of participants. Any set in Λ_{Qual} can recover the secret by stacking their transparencies and any set in Λ_{Forb} has no information on the shared image. They show constructions satisfying these requirements, with mild restrictions on the sets.

2.2.3 Extended VSS – Gray Scale

Naor & Shamir describe that many extensions from the basic work can be possible. Further they extend their work with following suggestions: Use partially filled circles to represent gray values. It is mentioned below in the following figure.

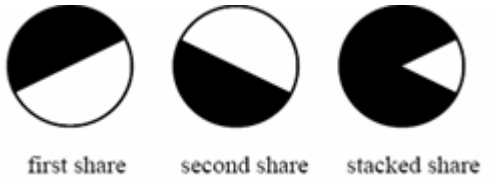

Figure 2.2: Extended VC Scheme

Above figure shows that for the continuous tone gray image we can use the pixels in the form of the circle. For example in above figure the superimposition of first two shares gives the third one. For the image dividing into the rotating circles as above it can give the color impression from gray color to black based on their adjustment or superposition. Example of the above extension is shown below.

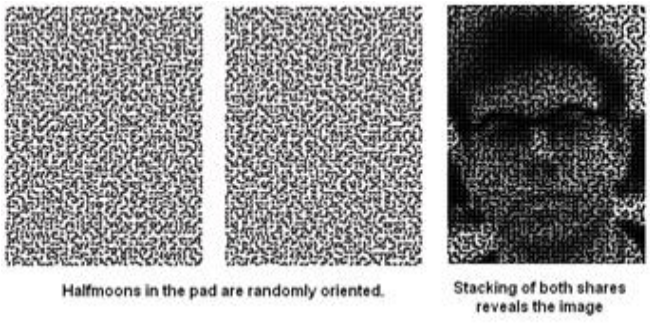

Figure 2.3: Example of the extended VC

Other extension as discussed by Naor and Shamir[2] is concealing the very existence of the secret data. In this scheme they consider the 2 x 2 array and take white if the two sub pixels are white (W) and two are black(B). Similarly take black if three sub pixels are black. This suggested scheme is shown below.

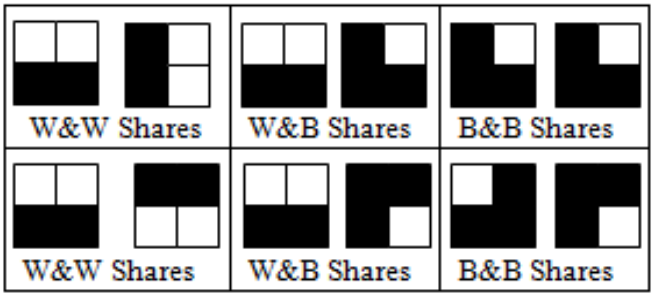

Figure 2.4. The basic idea of Noar and Shamir

Nakajima & Yamaguchi [16] have shown the results based on the implementation of their system that has used the extended visual cryptography scheme. Their system takes three images and gives two images. When stacked together the third image will be recovered.

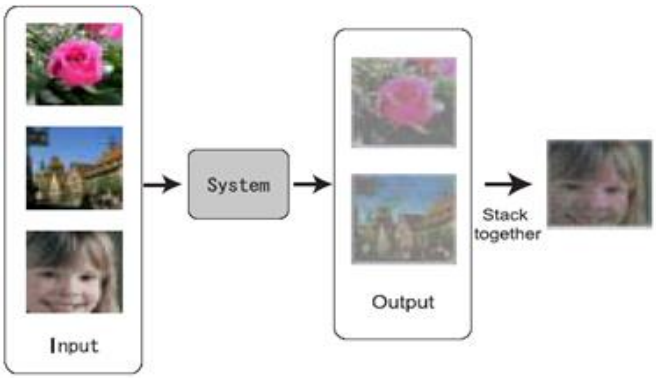

Figure 2.5. The system shows the basic idea of Extended VC

III. EXPERIMENTAL DESIGNS OF PROPOSED METHODS AND ILLUSTRATION

3.1 Randomized Visual cryptography scheme

We have designed some schemes on visual cryptography and visual secret sharing. Our approach for these schemes is randomization and pixel reversal. We have done several experiments and came up with some new approaches of (2, 2) visual cryptography and (3, 3) visual secret sharing schemes. First we explain the approach for the (2, 2) visual cryptography scheme.

In (2, 2) visual cryptography scheme we have one secret gray scale image (SI) as input to the algorithm. Here SI is considered as a matrix S_{ij} where i and j show pixel positions and i, j= 1, 2, 3,….., n. All steps of algorithm in this scheme are shown below.

Step1-

Pixel S_{ij} with position i and j is the input called original pixel.

Step2-

Apply pixel reversal i.e $S_{ij}' = 255 - S_{ij}$.

Step3-

Use random number generator (0.1 to 0.9) to reduce S_{ij}' randomly.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Step4-
Take the difference of S_{ij}' with original pixel S_{ij}.
Step5-
Use random number generator to reduce reversed value of S_{ij}' randomly.
Step6-
Apply pixel reversal i.e. $S_{ij}'' = 255 - S_{ij}'$.
Step7-
Store S_{ij}'' in matrix as image called share 1.
Step8-
Take the difference of two random number generators with original pixel S_{ij}.
Step9-
Apply pixel reversal i.e. $S_{ij}''' = 255 - S_{ij}'$.
Step10-
Store S_{ij}''' in matrix as image called share 2.
Step11-
epeat point 1 to 10 for all pixels from original image (i.e. matrix of original image)

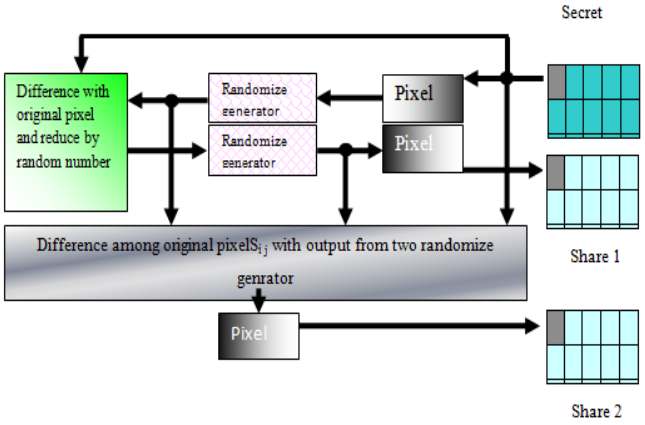

Figure 3.1. Randomize VC Scheme

This algorithm is shown in Figure 3.1. This VC scheme use gray scale secret image. In (2, 2) visual cryptography implemented by Naor & Shamir [3] the decoded image is twice that of original secret image because the pixel p expanded into two sub-pixels; this effect is called pixel expansion. This affects the contrast of the resulting image. The problem for the pixel expansion and contrast was discussed majorly in literature. The previous work on pixel expansion and contrast optimization shows that researchers did efforts to reduce the expansion and optimize the contrast of the secret picture. Further they portrait the process of creating the shares using mathematical representations and mainly they focus on the security and contrast condition.
In our scheme the decoded image is same in size of original secret message and there is no pixel expansion effect found. However the nature of the algorithm in general as with many other schemes result that the decrypted image is darker and contains a number of visual impairments. Our decoded secret image is darker then the original. The decoded secret image has increased the spatial resolution however most of visual cryptography schemes have shown the same effect in their decoded image.
After testing many different images from light to dark in resolution it was observed that the proposed algorithm could not take dark true image significantly with high contrast and then generate the meaningless shares. It is mostly found that the shares reveal the information. However on light contrast we have seen that the algorithm generates the perfect meaningless shares as shown in Figure 4.

3.2 Methodology

The approach of this paper uses meaningful shares (cover images) to hide the colored secret image and the recovery process here is lossless. This scheme defines a new stacking operation and requires a sequence of random bits to be generated for each pixel. This scheme is generalized to an *n* out of *n* approach. If we assume that a gray image with 256 colors constitutes a secret to be hidden then each color can be represented as an 8- bit binary vector.
The Secret image is broken up into 'k' shares and each share is encrypted with a cover image resulting into 'k' encrypted images. To recover the original image all the shares are to be stacked on top of each other.
The main idea is to expand each colored pixel into *m* subpixels and embed them into *n* shares. This scheme uses *m*=9 as an expansion factor. The resulting structure of a pixel can be represented by an n x 9 Boolean matrix $S=[Sij]$ where ($1 \le i \le n$, $1 \le j \le 9$) and Sij =1, if and only if, the jth subpixel in the ith share has a non-white color. To recover the color of the original secret pixel, an operation on the stacked rows of the *n* shares is performed.

3.2.1 Encryption Process

In the encryption Process, at first we convert the images (cover images) into matrix form. Then we read the pixel values of all the cover images and find out the ratio of them, according to the position. After this, the secret image values are broken according to this ratio values. Then each share is represented through binary forms. Next, we have to place (pixel value + 1) in the place of binary 1's. If the parts don't add up to the secret image pixel value add the remaining amount to the last part.
Algorithm:

1. Take the pixel values of all the cover images.
2. Find the ratio of the pixel values.
3. Break the secret image pixel value according to the ratio values.
4. Find the binary representation of each share.
5. Create the cover image sub-pixel by placing (pixel value + 1) in the position of binary 1's.
6. If the parts don't add up to the secret image pixel value add the remaining amount to the last part.

Illustration of Algorithm
Let the secret image pixel value be 96
Let the cover image (C1) pixel value be 38
Let the cover image (C2) pixel value be 5
Let the cover image (C3) pixel value be 72

Therefore,
The part in C1 = 38*96/(38+5+72) = 38*96/115 = 31
The part in C2 = 5*96/115 = 4
The part in C3 = 72*96/115 = 60
i.e. 31+4+60 = 95
Thus, C3 = 60+1 = 61

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Binary representation of the part in C1 = 000011111
Now, the cover image sub-pixel matrix of the first pixel value is produced by adding 1 to the pixel value where binary one appears. That is the matrix is

38	38	38
38	39	39
39	39	39

Binary representation of the part in C2 = 000000100 Sub-pixel matrix of the first pixel of the second cover image becomes

5	5	5
5	5	5
6	5	5

Binary representation of the part in C3 = 000111101 Sub-pixel matrix of the first pixel of the third cover image becomes

72	72	72
73	73	73
73	72	73

3.2.2 Decryption Process:

In the Decryption Process, we need to accept the encrypted cover images and read their sub-pixel values. Then we have to generate the binary value of the secret image pixel, by taking all pixel values as 0's and all (pixel value + 1) as 1's. Next, the binary number should be converted to decimal number. Finally, in order to get the actual secret image value, we need to add all the components.

Algorithm:

1. Accept the encrypted cover images and read the sub-pixel values.
2. Generate the binary value of the secret image pixel by
a. Considering all the pixel values to be 0's.
b. All the (pixel value + 1) values to be 1's.
3. Convert the binary number to decimal values.
4. Add all the components to generate the secret image pixel value.

Illustration of the Algorithm-
The pixels of the cover images are

38	38	38
38	39	39
39	39	39

C1

5	5	5
5	5	5
6	5	5

C2

72	72	72
73	73	73
73	72	73

C3

The binary numbers from the sub-pixels are:
C1 = 000011111 = 31
C2 = 000000100 = 4
C3 = 000111101 = 61
Therefore, the secret image pixel value is: 31+4+61 = 96.

IV. RESULTS AND DISCUSSION

The proposed algorithm was simulated and run on Matlab. The whole concept of our paper worked out is modeled below. This gives an overview of what we have done. It brings out a sophisticated model of our paper.

Figure 4.1(The MAIN Page)

Figure 4.2 (The ENCRYPTION Page)

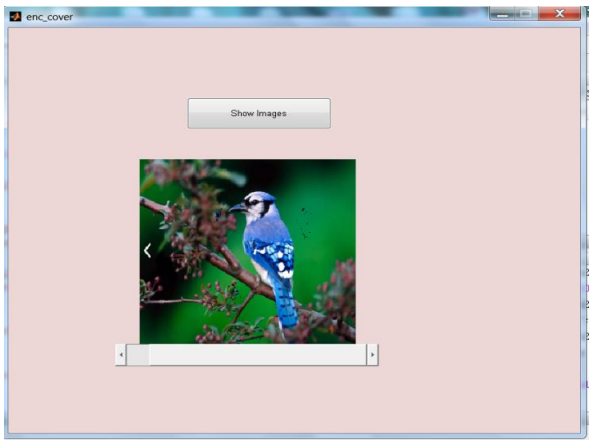

Figure 4.3 (Encrypted Image)

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

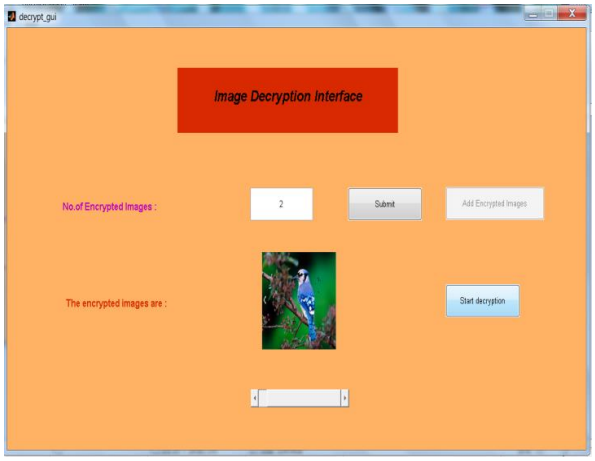

Figure 4.4 (The DECRYPTION Page)

Figure 4.5 (Decrypted Secret Image)

V. COMPARISON BETWEEN PREVIOUS WORK DONE AND OUR WORK

Previous Work Done

A lot of work on Visual Secret Sharing (V.S.S) Scheme has been done in the recent past [5]. The main difference in our work is that we are taking a steganographic approach to hide the data. This approach suggests that any outsider, if successful in obtaining the transmitted signal, fails to identify whether the data is in its original form or in an encrypted format.

One of the previous works involves the use of XOR operator to encrypt the images and using the binary values of the pixel to encrypt them. Thus it gave rise to the encrypted images with black spots all over the cover image. Following images are the examples of the previous work done:

Our Approach

In our approach we are dividing the secret image pixel value into the cover image pixel shares. Moreover we use the pixel value of similar order to hide the required data, thus making it a far better encryption process with a higher percentage of encryption and resolution. In our approach, the encrypted image appears to be in a much finer image quality with absolutely no spots in it. The encryption scheme in our approach results in the images of the following clarity.

Our Achievement towards the Goal

In this paper we presented a new technique based on an algorithm to hide a color secret image into two colored images. The generated camouflage images contain less noise and we achieved a considerable improvement in the Signal to Noise ratio (SNR) of the camouflage images by producing images with similar quality to the originals. This developed method does not require any additional cryptographic computations and achieves a lossless recovery of the secret image. In addition, the camouflage images obtained using this algorithm look less susceptible of containing a secret message. As future work, this scheme can possibly be modified to hide two independent colored secret images into n meaningful colored cover images. The recovery process of both secret images should remain lossless while using the same expansion factor as described in this presentation. A critical number has been determined which defines the number of cover images into which the secret image can be distributed resulting in encrypted images which cannot be distinguished visually from the original ones.

VI. SCOPE FOR FUTURE WORK

There is always a scope for further improvement in the work performed. The following points will provide a walk through the various aspects of the topics on which we would like to improve.

The points are:

1. The size of the encrypted image, if possible, should be decreased. It would help in speeding up the transmission of the encrypted images through the channel.
2. Insertion of a private key. This would help to provide two levels of encryption with personalized encryption process.

VII. CONCLUSION

In this paper we have tried to present an encryption and decryption process of a natural secret colour image into/from 'n' number of images based on Visual Secret Sharing Scheme.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

We have worked only on coloured images which are same in their dimensions. The encryption of a secret color image is done within two other cover colour images on the sender side. The decryption process of overlaying the two transparent sheets to produce the secret image has been realized in our work on the receiver side. The major improvement in our paper from previous works on this VSS Scheme is that the work in our paper can be expanded to be applied on (k,n) Visual Cryptographic scheme. So far, the works were done on the (2, 2) sharing basis. Thus by our work we could successfully send an image by encrypting it within two images, and successfully recovering the image back, which is a **lossless recovery.** The covered image is achieved without the loss of a single pixel. The scope of improvement in this paper lies in realizing and extending our paper goals by overcoming all the drawbacks, which we hope to achieve in our future days.

REFERENCES

1. Adi Shamir, "How to Share a Secret", published in ACM, Laboratory for Computer Science, Massachusetts Institute of Technology, 1979
2. Naor, M. and Shamir, A., "Visual cryptography", In Proc. Eurocrypt 94, Perugia, Italy, May 9–12, LNCS 950, pp. 1–12. Springer Verlag., 1994. http://www.wisdom.weizmann.ac.il/~naor/onpub.html.
3. Moni Naor, Adi Shamir, "Visual Cryptography" ,Lecture Notes in Computer Science, 1995, http://citeseer.ist.psu.edu/naor95visual.html.
4. Mizuho NAKAJIMA, Yasushi YAMAGUCHI, "Extended Visual Cryptography for Natural Images", Department of Graphics and Computer Sciences, Graduate School of Arts and Sciences, The University of Tokyo, 2002, http://wscg.zcu.cz/wscg2002/Papers_2002/A73.pdf
5. Harinandan Tunga," A New Secret Coloured Image Encryption and Decryption Scheme Based on Extended Visual Technology.
6. Verheul, E.R., van Tilborg, H.C.A., 1997 "Construction and Properties of k out of n visual secret sharing schemes" Designs Codes Cryptography. (11), 179–196.
7. C. Chang, C. Tsai, and T. Chen."A New Scheme For Sharing Secret Color Images In Computer Network", Proceedings of International Conference on Parallel and Distributed Systems, pp. 21–27,July 2000.
8. Chin-Chen Chang, Tai-Xing Yu, "Sharing A Secret Gray Image In Multiple Images", Proceedings of the First International Symposium on Cyber Worlds (CW.02), 2002.

Debabrata Bhattacharya has been with RCC Institute of Information Technology, Kolkata, India for the last thirteen years. He has a number of active research interest areas including image processing, computer architectures and data processing, measurements and communications. He has a vast international experience in computer industry and supervised several undergraduate dissertations. He did his B. Engg from Jadavpur University in 1983 and M. Tech from I.I.T Kharagpur in 1984, both in Electronics and Communication Engg.

Harinandan Tunga is with RCC Institute of Information Technology Kolkata, India for last nine years. His present research interests include Bioinformatics and Network Security. He has done B.Tech in 2003, ME in 2006. He has published ten papers in National & International conferences and Journals. He has supervised several undergraduate and postgraduate dissertations.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)