IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834, p- ISSN: 2278-8735.
PP 78-90
www.iosrjournals.org

A Stego Cryptography Algorithm for General Access Structures without Pixel Expansion

Soumya A M[1], Nitha S Unni[2]
[1](Electronics and Communication Engineering, SNGCE/M G University,India)
[2](Electronics and Communication Engineering, SNGCE/M G University,India)

Abstract : *Visual secret sharing schemes generate noise-like random pixels on shares to hide secret images. It suffers a management problem, because of which dealers cannot visually identify each share. This problem is solved by the extended visual cryptography scheme which adds a meaningful cover image in each share. However, the previous approaches involving the EVCS for general access structures suffer from a pixel expansion problem. In this paper, we propose a general approach to solve the management and pixel expansion problems; the approach can be used for binary secret images in non computer-aided decryption environments. The proposed approach consists of two phases. In the first phase, based on a given access structure, we construct meaningless shares. In the second phase, cover images are added in each share directly by a stegnography algorithm using DCT. The experimental results indicate that a solution to the pixel expansion problem of the EVCS for GASs is achieved.Also the management problem is overcome by adding cover image by using steganography. Moreover, the display quality of the recovered image is very close to that obtained using conventional VC schemes.*

Keywords – *Extended visual cryptography,General access structures,Stegnography,Visual secret sharing scheme.*

I. INTRODUCTION

Visual Cryptography (VC), which was proposed by Naor and Shamir, allows the encryption of secret information in the image form[1]-[2]. By applying the concept of secret sharing, a secret image can be encrypted as *n* different share images printed on transparencies, which are then distributed to participants. By stacking transparencies (shares) directly, the secret images can be revealed and visually recognized by humans without any computational devices and cryptographic knowledge. On the other hand, any one share or a portion of shares can leak nothing related to the secret image. VC is a very good solution for sharing secrets when computers cannot be employed for the decryption process.

Visual Cryptography Scheme (VCS) is an encryption method that uses combinatorial techniques to encode secret written materials.The idea is to convert the written material into an image and encode this image into n shadow images. The decoding only requires only selecting some subset of these n images, making transparencies of them, and stacking them on top of each other. In the past decade, many research results on the threshold visual secret sharing scheme (also known as k-out-of-n VSS scheme or (*k, n*) -VSS scheme) have been proposed.

In general, a (*k, n*) secret sharing scheme is a method to share a secret K among n participants such that the following conditions hold:Any k participants together can compute K.Any *t* participants, $t < k$, gain no information about K. Here is an example of a $(2,2)$ secret sharing scheme[3]-[10]. Assume that the secret K is a binary sequence of length *m*, i.e. $K = (k_1, k_2, \ldots \ldots, k_m)$. The two shares, s_1 and s_2 can be constructed as follow. The first share is chosen to be a random binary sequence of length m, say $s_1 = (s_{11}, s_{12}, \ldots \ldots, s_{1m})$. Then, we can compute the second share by doing "exclusive-or" on K and s_1

$$s_{2i} = k_i \oplus s_{1i, i=1 \ldots \ldots m} \quad (1.1)$$

$$s_{2i} = k_i \oplus s_{1i}, i = 1 \ldots \ldots m \quad (1.2)$$

For example, assume that $m = 2$, $k = (0,1)$. Then the two shares can be constructed as follow:

$s_1 = (0,0)$, then $s_2 = s_1 \oplus K = (0,1)$.
$s_1 = (0,1)$,then $s_2 = s_1 \oplus K = (0,0)$.
$s_1 = (1,0)$, then $s_2 = s_1 \oplus K = (1,1)$.
$s_1 = (1,1)$, then $s_2 = s_1 \oplus K = (1,0)$.

However, looking only at one share, say S_1, any four values of K are possible. In other words, it gains no information about K if another share S_2 is unknown. Ateniese *et al.* (denoted as Ateniese in[11] short proposed the concept of general access structure (GAS) and also developed a VC-based solution for some GASs[12]. Afterward, Hsu *et al.* reported the formulation of an unexpanded VCS for a GAS problem.Liu *et al.* (denoted as Liu in short) proposed a recursive approach to construct VCS for GASs. By using the GAS, dealers can define reasonable combinations of shares as decryption conditions rather than specifying the number of shares. For example, if there are four participants-one CEO, one manager, and two employees-sharing a secret, the CEO may expect to decrypt the secret with any one colleague who holds one of the other shares. The manager is allowed to obtain the secret with only two employees. The two employees are restricted access to the secret. Due to these flexibilities, dealers can also set the number of shares as the decrypting condition. Hence, the (*k*,*n*) VSS scheme can be treated as a special case of the GAS.

Conventional VSS schemes generate noise-like random pixels on shares to hide secret images. In this manner, the secret can be perfectly concealed on the share images. However, these schemes suffer from a management problem,dealers cannot identify each share visually. Hence, researchers have developed the extended visual cryptography scheme (EVCS, also known as the friendly VC scheme), which adds a meaningful cover image on each share to address the management problem. Ateniese presented a general technique to implement (*k*,*k*) -threshold EVCS as well as various interesting classes of access structures for binary secret images. Fang and Chen *et al.* proposed VC-based and random-grid based techniques, respectively, for (*k*,*k*)–EVCS with[13]-[14] a progressive decryption effect. Wang *et al.* developed a matrix extension algorithm for(*k*,*n*) -EVCS by modifying any existing VCS with random-looking shares, which were then utilized as meaningful shares.

The pixel expansion problem is a common disadvantage with most of the VSS schemes. When the VC-based approach is employed, each secret pixel within a secret image is encrypted in a block consisting of subpixels in each constituent share image. Thus, the area of a share is *m* times that of the original secret image. The contrast of the recovered images will be decreased to 1/*m* simultaneously[1].The pixel expansion problem not only affects the practicability of storage/transmission requirements for shares but also decreases the contrast of the recovered secret images. To the best of our knowledge, the existing EVCS algorithms for GASs cannot avoid the pixel expansion problem.

In this paper, we propose a novel encryption algorithm of EVCS for general access structures to cope with the pixel expansion problem. The proposed algorithm is applicable to binary secret/cover images, and no computational devices are needed during the decryption phase. In order to avoid pixel expansion, we do not adopt the traditional VC-based approach to encrypt secret images. The encryption process can be divided into two phases. The first phase of the algorithm, for a given access structure, constructs a set of noise-like shares that are pixel-expansion-free. The second phase of the algorithm directly adds a cover image on each share via a stegnographic algorithm.

Steganography is the art and science of invisible communication of messages. This is done by hiding information in other information, ie. hiding the existence of the communicated information[16]-[17]. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”. In image steganography the information is hidden in images. The idea and practice of hiding information has a long history. In Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave’s scalp. When the slave’s hair grew back the slave was dispatched with the hidden message. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.

Cryptography is a technique for securing the secrecy of communication. Many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Sometimes it is not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. Steganography is the technique used for implementing this. The difference between Steganography and Cryptography is that the cryptography focuses on keeping the contents of a message secret whereas steganography focuses on keeping the existence of a message secret. Steganography and cryptography[15]-[17] both are ways for protecting information from unwanted parties.

The basic LSB based technique simply replaces the LSB plane of the carrier image with the bit stream of secret information. These methods are based on false assumption that LSB plane of natural images is random enough, thus are suitable for data hiding. In this paper, we propose a technique based on Least Significant Bits replacement considering DCT coefficient value of pixels. The DCT of[18] carrier image is obtained then based on proper threshold random locations are selected. LSBs of these potential locations in carrier image are replaced with MSBs of the secret image.

II. Background And Related Work

1.Visual secret sharing scheme

Naor and Shamir proposed a visual secret sharing scheme (VSSS) that uses human visual system to decrypt the secret image without performing any cryptographic computation. The difference between a VSSS and a traditional secret sharing scheme is in how the secret is decrypted. Usually, the traditional secret sharing scheme requires computation over a finite field. In a VSSS, however, the computation is simply performed by the human visual system of the users.

It is important to realize that the construction of a secure VSSS is difficult. Suppose that a particular pixel P on a share S_i is black. Whenever a set of shares (including S_i) is stacked together, the result must be black. It means that in the secret image, the pixel P must be black. In other words, we gain "some" information about the secret image be examining one of the shares, and the security condition does not allow this. Naor and Shamir proposed a VSSS that solved this problem by splitting each original pixel into *m* subpixels. In this section, we will introduce this idea and explain how to decrypt "visually".In general, a VSSS assumes that the secret is a collection of black and white pixels, or a binary image, and each pixel is encrypted separately. Figure1&2 show the details. Each original pixel encrypts into *n* shares, and each share is a collection of *m* black and white subpixels, which are printed near to each other such that human visual system averages their individual black/white contribution. The VSSS can be described by an $n \times m$ Boolean matrix M where $M[i, j] = 1$ iff the *j*-th subpixel in the *i*-th shares is black, and $M[i, j] = 0$ iff the *j*-th subpixel in the *i*-th shares is white.

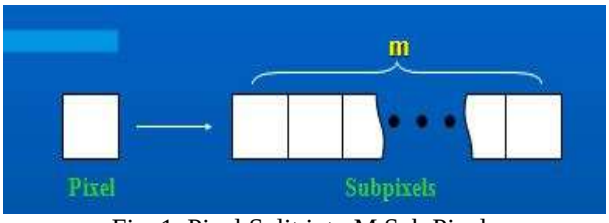

Fig. 1. Pixel Split into M Sub Pixels

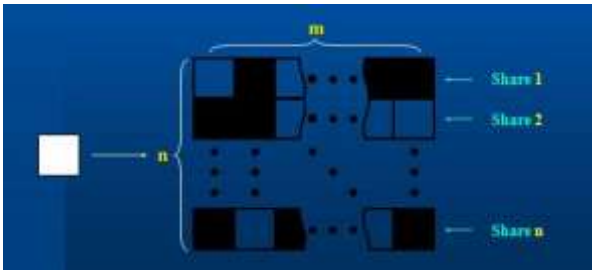

Fig.2. N Shares Per Pixel

2. A general (k,k) vsss

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).

3. General access structure scheme

Ateniese, Blundo, Santis and Stinson extend the VSSS to a general access structure VSSS. Here is an example to illustrate the idea. Assume that a bank has a vault. In this time, the bank employs three senior tellers and a manager. They would like to design a system such that one of the three senior tellers together with the manager can open the vault. However, two of the three senior tellers can not obtain the permission. This problem can be viewed as a general access structure scheme.

In a (*k*,*n*) VSSS, the secret image is decrypted by stacking any *k* shares together. In a general access structure VSSS, however, we can specify some qualified subsets of shares that can decrypted the secret image, but other forbidden subsets of shares have no information about the it. For example, assume that there are four shares. Let P={S_1,S_2,S_3,S_4} be the set of all shares, and let 2^P denotes the set of all subsets of P. Suppose that we want to construct a VSSS such that the qualified sets are all subsets of P containing at least one of the three sets, (S_1,S_2),(S_2,S_3) or (S_3,S_4). In order words S_1,and S_2, together can decrypt the secret, so as (S_2,S_3) and (S_3,S_4). Hence, the family of qualified sets is

$$\Gamma_{Qual} = \{(S_1,S_2),(S_2,S_3),(S_3,S_4),(S_1,S_2,S_3),(S_1,S_2,S_4),$$
$$(S_1,S_3,S_4),(S_2,S_3,S_4)(S_1,S_2,S_3,S_4)\}$$

Let all remaining sets of P be the forbidden sets.

$$\Gamma_{Forb} = \{(S_1),(S_2),(S_3),(S_4),(S_1,S_3),(S_1,S_4),(S_2,S_4)\}$$

The pair ($\Gamma_{Qual},\Gamma_{Forb}$) is called the access structure of the scheme.

4. Image steganography techniques

Based on the analyses of steganography tools' algorithms, we partition these tools into two categories:

(1) Spatial domain based steganography

(2) Transform domain based steganography.

5. Spatial Domain Based Steganography

Spatial steganography mainly includes LSB (Least Significant Bit) steganography Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image . The leas t significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. Figure 3&4 shows the examples for cover image and stego image.

Pixel: (10101111 11101001 10101000)
(10100111 01011000 11101001)
(11011000 10000111 01011001)

Secret message: 01000001

Result: (10101110 11101001 10101000)
(10100110 01011000 11101000)
(11011000 10000111 01011001)

Fig.3. Cover Image

Fig. 4. Stego Image

6.Ttransform domain based steganography

Basically there are many kinds of power level transforms that exist to transfer an image to its frequency domain, some of which are Discrete Cosine Transform, KL Transform and Wavelet Transform.

7. The Discrete Cosine Transform (DCT)

This method is used, but similar transforms are for example the Discrete Fourier Transform (DFT). These mathematical transforms convert the pixels in such a way as to give the effect of "spreading" the location of the pixel values over part of the image. The DCT transforms a signal from an image representation into a frequency representation, by grouping the pixels into 8 × 8 pixel blocks and transforming the pixel blocks into 64 DCT.

DCT 11100 is used in steganography as- Image is broken into 8×8 blocks of pixels. Working from left to right, top to bottom, the DCT is applied to each block. Each block is compressed through quantization table to scale the DCT coefficients and message is embedded in DCT coefficients..

8. Existing System

There are many extensions and improvements of the basic VSSS exists. For a $(2,2)$ VSSS, a pixel is interpreted by the visual system. there is 50% loss of contrast in the decrypted image. For (k,k) VSSS, the contrast loss will be much more serious as k become larger. Therefore, the construction method to improve the contrast is required. Since the share image looks like a random noise. It makes everyone know that there are some secret hidden under the share image. It might be useful to conceal the share image under innocent images. The pixel expansion problem is a common disadvantage with most of the VSS schemes. When the VC-based approach is employed, each secret pixel within a secret image is encrypted in a block consisting of subpixels in each constituent share image. Thus, the area of a share is m times that of the original secret image. The contrast of the recovered images will be decreased to 1/m simultaneously. The pixel expansion problem not only affects the practicability of storage/transmission requirements for shares but also decreases the contrast of the recovered secret images. To the best of our knowledge, the existing EVCS algorithms for GASs cannot avoid the pixel expansion problem.

III. PROPOSED SYSTEM

This system present a two-phased encryption algorithm of (IQ,Iforb) EVCS for GASs. In the first phase, it generates intermediate shares of VCS. These intermediate shares (I-shares) have a meaningless appearance and no pixel expansion. In the second phase, cover images will be added in these I-shares to yield the resultant shares.

1. Advantages of Proposed System

One of the advantage is the modularity. Each phase in the encryption procedure is less coherent, so it can be individually designed and also can be replaced separately.Over all system security is increases.Pixel expansion problem is reduced.

2.Proposed Encryption Algorithm

In this section, we present a two-phased encryption algorithm of $(\Gamma_{Qual}, \Gamma_{Forb})$-EVCS for GASs. The solution procedures are shown in Fig. 5. In the first phase, it generates intermediate shares (i.e. $I_1 \ldots\ldots\ldots\ldots I_n$,

in Fig.5) of $(\Gamma_{Qual},\Gamma_{Forb})$-VCS. These intermediate shares (I-shares) have a meaningless appearance and no pixel expansion. In the second phase, cover images will be added in these I-shares to yield the resultant shares of $(\Gamma_{Qual},\Gamma_{Forb})$-EVCS (i.e. $P_1 \dots \dots \dots \dots P_n$, in Fig.5). Each module in Fig.5 will be described in the following section.

3. Phase I: Generating I-Shares

This phase aims to construct a pixel expansion free VCS for a given access structure $(\Gamma_{Qual},\Gamma_{Forb})$. The main idea behind the solution approach is as follows. A security system employs n' different keys to protect a secret and distributes these keys to *n* participants. Each key may be duplicated and will be distributed to at least one participant. Each participant is allowed to hold at least one key. Considering this scenario, if someone wants to access the secret, he/she has to collect n' different keys from a set of participants. If he/she misses any one type of key, the secret will remain protected. To construct such a security system for an access structure $(\Gamma_{Qual},\Gamma_{Forb})$, the dealer has to carefully distribute n' different keys to any set of participants $X, X \in \Gamma_{Qual}$, and has to guarantee that any set of participants $Y, Y \in \Gamma_{Forb}$, will not hold all types of keys. Hence, the method of distribution of n' different keys to *n* participants will provide a solution for a given access structure.

For example, there are 4 participants $P = \{i_1, i_2, i_3, i_4\}$, sharing a secret image upon the qualified set $\Gamma_{Qual} = \{\{i_1, i_2, i_3, i_4\}\}$and the forbidden set $\Gamma_{Forb} = 2^P \backslash \Gamma_{Qual}$. Intuitionally, we can utilize the construction of a (4,4)-VCS to yield 4 shares s_1, s_2, s_3 and s_4 (called basis shares), and then distribute one basis share to each participant. For example, participant i_1 holds the share s_1, i_2 holds the share s_2, and so on. Finally, we have 4 I-shares $I_1 \dots \dots \dots \dots I_4 (I_1 = \{s_1\} \dots \dots \dots I_4 = \{s_4\})$ for the $(\Gamma_{Qual},\Gamma_{Forb})$-VCS. Obviously, upon stacking I-shares I_1, I_2, I_3 and I_4 (according to $\Gamma_{Qual} = \{\{i_1, i_2, i_3, i_4\}\}$), the secret image which is the same as the result of the (4,4)-VCS, can be revealed.

In this paper, construction of n', n' -VCSs is adopted to be the encryptor in Fig. 4.1. The I-shares of a $(\Gamma_{Qual},\Gamma_{Forb})$–VCS are synthesized from the basis shares that are the products of the encryptor. The construction set C holds the relation between the basis shares and the I-shares.

Definition 1: Assume that the n', n'-VCS, where $n' \geq 2$ is to be used to construct a $(\Gamma_{Qual},\Gamma_{Forb})$-VCS with *n* participants $P = \{i_\alpha, 1 \leq \alpha \leq n\}, n \geq 2$. Construction set *C* denotes the constitution member of *n* shares of the $(\Gamma_{Qual},\Gamma_{Forb})$-VCS, c_α represents the constitution member of participant $i_\alpha, c_\alpha = \{s_j, 1 \leq j \leq n'\}$, $c_\alpha \in C$. Basis share s_j, $1 \leq j \leq n'$, is the resultant share of the (n', n')-VCS. Shares of participant i_α can be defined as . $I_\alpha = U_{\forall s,} \in c_\alpha s_j$. By Definition 1, the construction set of the above example can be expressed as $C = \{\{s_1\}, \{s_2\}, \{s_3\}, \{s_4\}\}$. As black and white pixels are presented by logical "1" and "0," respectively, the stacking shares will be limited in pixel-wise "OR"-ed operation. Hence, the recovered image for $\Gamma_{Qual} = \{\{i_1, i_2, i_3, i_4\}\}$ should be the stacking result of s_1, s_2, s_3 and s_4 which is the same as that of the (4,4)-VCS. In summary, phase I of the proposed algorithm contains two subprocedures: first, finding the number of basis shares n' and a corresponding construction set *C* for a $(\Gamma_{Qual},\Gamma_{Forb})$-VCS. We develop a GAS selector, as shown in Fig.5, to deal with these works.

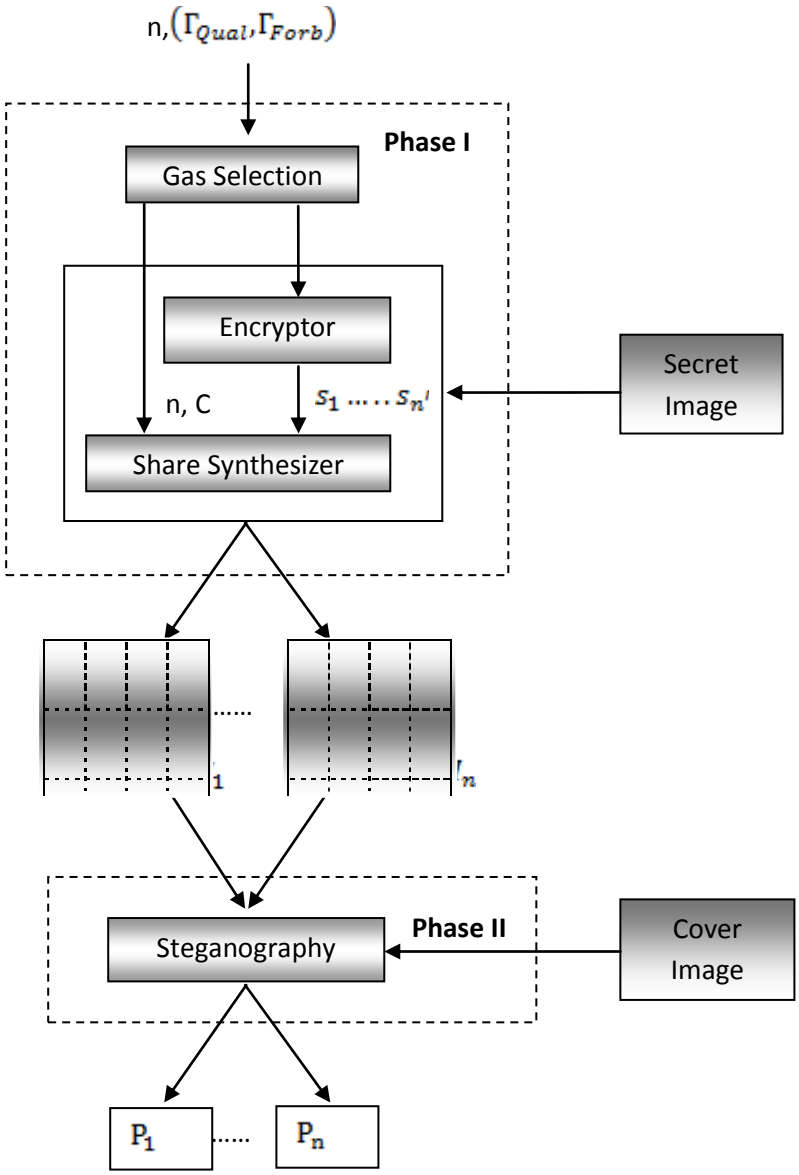

Fig.5. Block Diagram Of Encryptor and the Share Synthesizer

4. Phase II:Adding Cover Images

In this section, we have proposed adding cover images on I-shares, that were produced in the first phase. There are two major differences between our approach and the existing research for the EVCS. First, we put cover images on shares directly. Hence, our approach does not introduce any pixel expansion in this phase. Second, the black pixel density of the cover images can be adjusted on demand in a fine-grained fashion.For adding cover images we use Stegnography.

In this section, we first present a brief overview of basic LSB based technique and then will enhance the selection criteria for potential locations by using DCT coefficients. Further the embedding and retrieval process will be explained using image examples.In basic LSB based technique, the bits from secret image simply overwrite LSBs, i.e. maximum four least significant bits of the carrier image, while other higher order bit planes are preserved. Embedding data in higher bit planes may sometime results in visible artifacts in the stego image. It is only because of image contents and can be avoided by proper selection of carrier image. The Discrete Cosine Transform (DCT) transforms the image from spatial domain to frequency domain. It separates

the image into spectral sub-bands with respect to its visual quality, i.e. high, middle and low frequency components.

In DCT based techniques, DCT coefficients are obtained for the given carrier image. The secret data is embedded in the carrier image for DCT coefficients lower than the threshold value. To avoid visual distortion, embedding of secret information is avoided for DCT coefficient value 0. Insertion and extraction of secret image is an important part for any steganographic technique. Algorithm for embedding and retrieval of secret image are given here.

5. Dct Based Steganography

5.1Algorithm To Embed Text Message:-

Step 1: Read cover image.
Step 2: Read secret message and convert it in binary.
Step 3: The cover image is broken into 8×8 block of pixels.
Step 4: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 5: DCT is applied to each block.
Step 6: Each block is compressed through quantization table.
Step 7: Calculate LSB of each DC coefficient and replace with each bit of secret message.
Step 8: Write stego image.

5.2 Algorithm To Retrieve Text Message:-

Step 1: Read stego image
Step 2: Stego image is broken into 8×8 block of pixels.
Step 3: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 4: DCT is applied to each block.
Step 5: Each block is compressed through quantization table.
Step 6: Calculate LSB of each DC coefficient

6. Steganography

Steganography is the process of hiding the secret messages or its existence so that it remains unidentified or undetected**.**The strong steganography should follow certain properties such as capacity-it should be capable of hiding information.Block diagram for stegaocryptography algorithm is shown as in figure 6.

The procedure for data hiding using steganographic algorithm is as follows:

1) We first use the steganographic algorithm for encrypting the secret message.

2) For this encryption, the we uses any text documents or audio or video files in which the data is written and the image file as a carrier file in which the secret message or text document or audio or video file to be hidden.

3) The carrier file and text document or audio or video file gives to the encryption phase for data embedding, in which the text document or audio or video file is embedded into the image file..

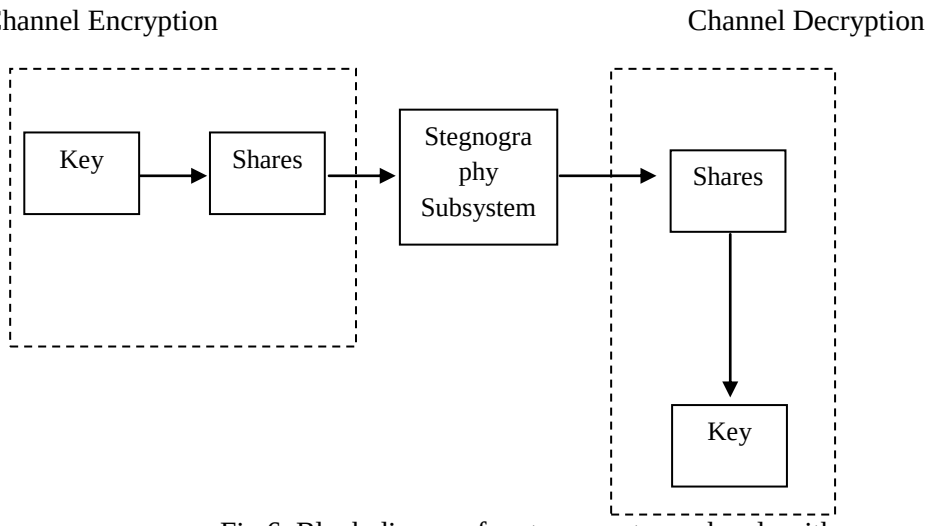

Fig.6..Block diagram for stegocryptography algorithm

The procedure for data hiding using stego cryptographic algorithm is as follows:

1) First we select the secret key
2) Generate different shares
3) Adding cover image using steganography
4) Retrieve the data by extracting the shares

Stego cryptography is the combined form of cryptography and steganography.Combining both cryptography and steganogrphy methods used to enhance the security.

7. Cryptography

Cryptography defines the art and science of transforming data into a sequence of bits that appears as random and meaningless to a side observer or attacker.Block diagram for cryptography is shown as in figure 7.In this in sender section we first select the key image then choose GAS. Then convert it into shares.In receiver section select the corresponding shares and finally we get the key image. select the key image then choose GAS. Then convert it into shares.In receiver section select the corresponding shares and finally we get the key image.

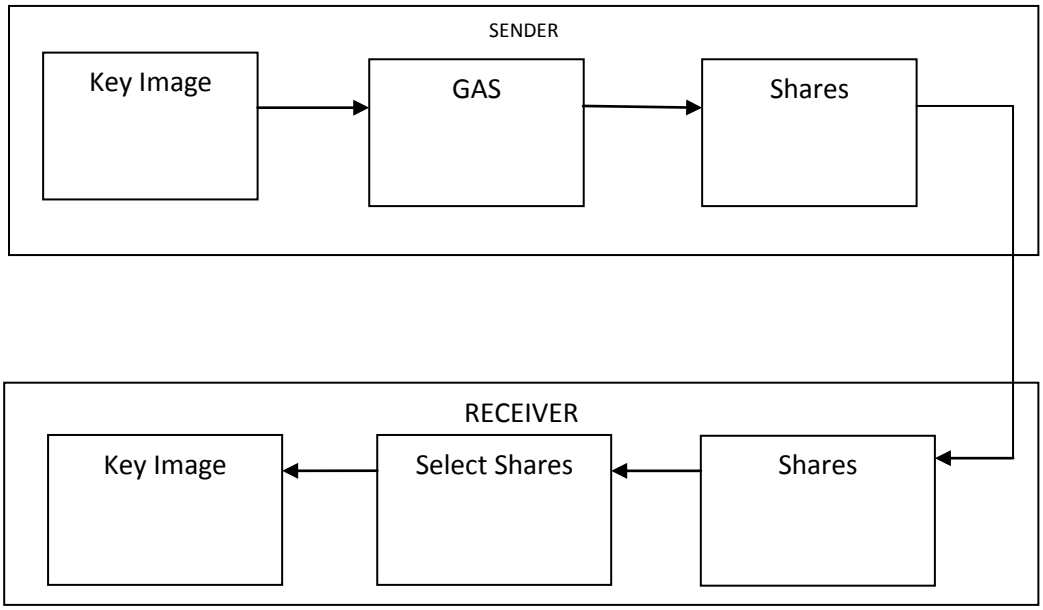

Fig.7.Block diagram for cryptography

In encryption phase, the data is embedded into carrier file which was protected with the password. Now the carrier file acts as an input for the decryption phase. The image in which data is hidden i.e. the carrier file is using a transmission medium. E.g. Web or e-mail. Finally get the carrier file and places the image in the decryption phase. In the decryption phase, the original text document or audio or video file can be revealed using the appropriate password. The decryption phase decrypts the original text document or audio or video file using the least significant bit decoding and decrypts the original message. As mentioned in the above block diagram, the data hiding and the data extracting will be done in three phases.

8. Hiding Share Image In Host Images

This is the encryption phase.It uses two types of files for encryption purpose. One is the secret file which is to be transmitted securely, and the other is a carrier file such as image. In the encryption phase the data is embedded into the image using "Least Significant Bit algorithm" (LSB) by which the least significant bits of the secret document are arranged with the bits of carrier file such as image, Such that the message bits will merge with the bits of carrier file. In this procedure LSB algorithm helps for securing the originality of image. Figure 8. shows the details.

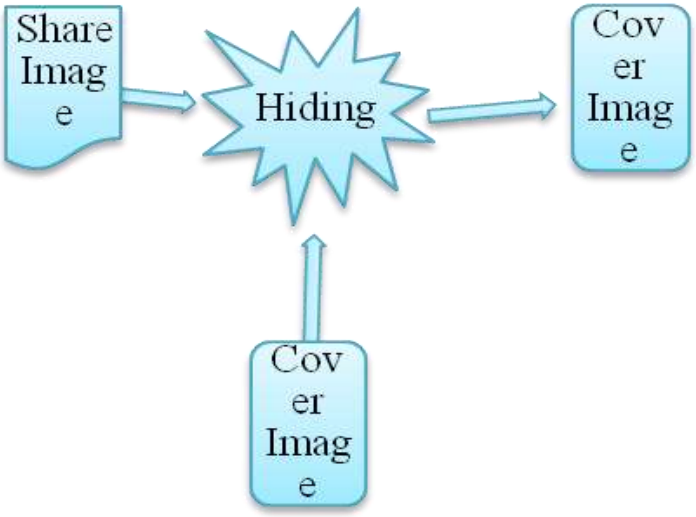

Fig. 8. Block Diagram for Encryption Phase

9.Extract Share Image From Host Image

It is the decryption phase.It is reverse to encryption phase. In this phase, the carrier image in which the data is hidden is given as an input file. The decryption phase uses the same password which was given for the encryption and decryption in order to secure from unauthorized access. After giving the correct password the decryption section uses the "Least Significant bit Algorithm" (LSB) by which the encoded bits in the image is decoded and turns to its original state and gives the output as a text document or audio or video file as well as image. Figure 9.shows the block diagram of Decryption

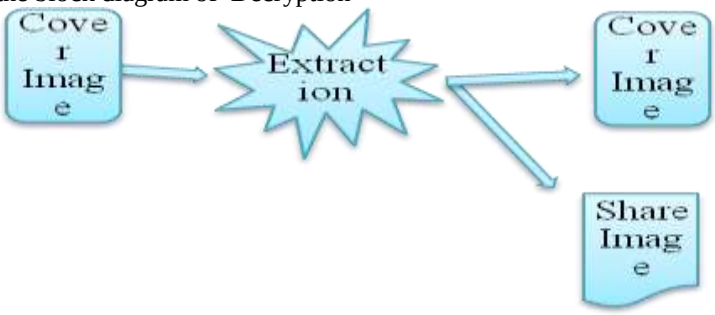

Fig:9. Block Diagram for Decryption Phase

IV. Result And Analysis

In this section, we evaluate the performance of the proposed model. Then, we assess the performance of the proposed encryption algorithm for Stego Cryptography in terms of the contrast of the recovered secret images. Finally,the results of our implementation of Stego Cryptography can avoid the pixel expansion problem and the management problem.Figure 10-15 shows the proposed model for stego cryptography algorithm.

Fig.10.Proposed System

Fig.11.Browsing Image

Fig12.Selection of Secret Key

Fig.13.Adding Cover Image

Fig.14.Extracting Shares

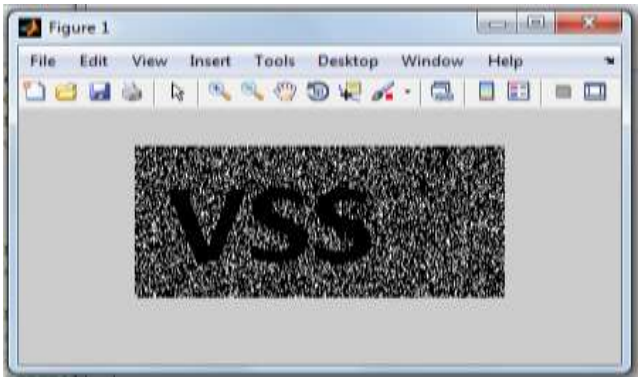

Fig.15.Secret Image From Shares

V. Conclusion

In this paper, we have proposed a two-phased encryption algorithm for the EVCS for general access structures. From the point of view of pixel expansion, our approach successfully solves the open questions. The experimental results also show that in most of the cases, our approach has better performances than those proposed in previous research in terms of the display quality of the recovered image, which includes contrast, perfect reconstruction of black secret pixels, and maintenance of the same aspect ratio as that of the original secret image. The proposed algorithm has several advantages. First, the algorithm is a generic approach.. The second advantage is the modularity. Each phase in the encryption procedure is less coherent, so it can be individually designed and also can be replaced separately. The third advantage is the first phase of the proposed algorithm: this phase is applicable not only to the extended VC schemes but also to the conventional VC schemes.The major contributions of our work are as follows.This is the first solution that addresses the pixel

problem of the EVCS for general access structures. By adopting the proposed steganography algorithm, all existing VC schemes can be modified to form their extended VC schemes. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. It is therefore a book on magic. It is emerging in its peak because it does not attract anyone by itself. In this paper analysis of DCT method has been successfully implemented and results are delivered. Thus by using the stego cryptography algorithm for general access structures without pixel expansion we have to increase the system security to a high level.

References

[1]. Kai-Hui Lee and Pei-Ling Chiu,"An Extended Visual Cryptography Algorithm For General Access Structures ", vol. 7, no. 1, february 2012, IEEE transactions on information forensics and security.
[2]. M. Naor and A. Shamir, "Visual cryptography," in Proc. Advances in Cryptology (Eurprocrypt'94), 1994, pp. 1–12.
[3]. E. R. Verheul and H. C. A. v. Tilborg, "Constructions and propertiesof k-out-of- n visual secret sharing schemes," Designs Codes Crypto., vol. 11, pp. 179–196, 1997.
[4]. H. Koga, "A general formula of the (t,n)-threshold visual secret sharing scheme," in Proc. Advances in Cryptology (Asiacrypt), 2002, pp. 328–345.
[5]. A. Adhikari and S. Sikdar, "A new (2, n)-visual threshold scheme for color images," in Proc. INDOCRYPT 2003, Berlin, Germany, 2003, pp 148–161.
[6]. C. Blundo, P. D'Arco, A. D. Santis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," SIAMJ Discrete Math., vol. 16, pp. 224–261, 2003.
[7]. C. N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognit. Lett., vol. 25, pp. 481–494, 2004.
[8]. C. Blundo, S. Cimato, and A. D. Santis, "Visual cryptography schemes with optimal pixel expansion," Theor. Comput. Sci., vol. 369, pp. 169–182, 2006.
[9]. D. Wang, L. Zhang, N. Ma, and X. Li, "Two secret sharing schemes based on boolean operations," Pattern Recognit., vol. 40, pp. 2776–2785, 2007.
[10]. P. L. Chiu andK.H.Lee, "Asimulated annealing algorithm for general threshold visual cryptography schemes," IEEE Trans. Inf. Forenics Security,vol. 6, no. 3, pp. 992–1001, Sep. 2011.
[11]. G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Visual cryptography for general access structures," Inform. Comput., vol. 129, pp. 86–106, 1996.
[12]. F. Liu, C. Wu, and X. Lin, "Step construction of visual cryptography schemes," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 27–38, Mar. 2010.
[13]. W. P. Fang, "Friendly progressive visual secret sharing," Pattern Recognit., vol. 41, pp. 1410–1414, Apr. 2008.
[14]. T. H. Chen and Y. S. Lee, "Yet another friendly progressive visual secret sharing scheme," in Proc. 5th Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing, 2009, pp. 353–356.
[15]. G.Ateniese,C.Blundo,A.D.Santis,andD.R.Stinson,"Extended capabilities for visual cryptography,"Theor. Comput. Sci., vol. 250, pp. 143–161, 2001.
[16]. Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav "Steganography Using Least Signicant Bit Algorithm" ISSN: 2248-962 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp. 338-341 338
[17]. Hardik Patel, Preeti " Steganography techniqueBased on DCT Coefficients".ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 1,Jan-Feb 2012, pp.713-717 713
[18]. Gurmeet Kaur and Aarti Kochhar"Steganography Implementation based on LSB & DCT" International Journal for Science and Emerging ISSN No. (Online):2250-3641 Technologies with Latest Trends" 4(1): 35-41 (2012) ISSN No. (Print): 2277-8136