ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

Multiple Secret Sharing Using Half Toning

V.Chinnapu Devi, S.Nikitha, M.Mahesh, Shaik. Moulali

Assosciate Professor, Dept. of ECE, Brindavan Institute of Technology & Science, Kurnool, India

B.Tech Student, Dept. of ECE, Brindavan Institute of Technology & Science, Kurnool, India

B.Tech Student, Dept. of ECE, Brindavan Institute of Technology & Science, Kurnool, India

B.Tech Student, Dept. of ECE, Brindavan Institute of Technology & Science, Kurnool, India

***ABSTRACT*:** A conventional threshold (k out of n) visual secret sharing scheme encodes one secret image into transparencies (called shares) such that any group of k transparencies reveals when they are superimposed, while that of less than k ones cannot. We define and develop general constructions for threshold multiple-secret visual cryptographic schemes (MVCSs) that are capable of encoding s secret images P1,P2,P3.......Ps into n shares such that any group of less than k shares obtains none of the secrets, while 1) each group of k, k+1,......n shares reveals P1P2,........Ps, respectively, when superimposed, referred to as(k,n,s) -MVCS where s=n-k+1; or 2) each group of u shares reveals P_{r_u} where r_u€{0,1,2,.......s}(r_u= 0indicates no secret can be seen), and, referred to as(k,n,s,R) -MVCS in which is called the revealing list. We adopt the skills of linear programming to model and MVCSs as integer linear programs which minimize the pixel expansions under all necessary constraints. Our constructions are novel and flexible. They can be easily customized to cope with various kinds of MVCSs.

KEYWORDS: linear programming, multiple secrets, pixel expansion, threeshold visual secret sharing.

I.INTRODUCTION

When secret information is managed by individuals, there exist potential treats of interruption, interception, modification and/or fabrication owing to inadequate management, natural disasters or human attacks (by malicious intruders or unfaithful individuals). Thus, the design of secret sharing approaches that allow the secret to be shared among a group of participants has become a significant and vital research topic in modern security. The concept of threshold secret sharing was first proposed by Shamir and Blakely [4] independently in 1979. A threshold secret sharing scheme encodes a secret into shares, which are distributed to the participants, such that only any group of k (or more) participants can decode using their shares, while that of less than ones cannot in an information-security concern.. Therefore, the secret is not only safeguarded from all groups of less than k shares, but also tolerant of a loss of up to n-k ones.

Visual cryptography was originally invented and pioneered by Noor and Shamir in 1994 at the eurocrypt conference. Visual cryptography is “a new type of cryptography scheme, which can decode concealed images without any cryptographic computation”. As the name suggests, visual cryptography is related to the human visual system. When the k shares are stacked together, the human eye does the decryption. This allows anyone to use the system without any knowledge of cryptography and without performing any computations whatsoever. This is another advantage of visual cryptography over the popular conditionally secure cryptography schemes. The mechanism is very secure and very easily implemented. An electronic secret can be shared directly; alternatively the secrets can be printed out on to transparencies and super imposed, revealing the secret.

Naor and Shamir’s initial implementation assumes that the image or message is a collection of black and white pixels, each pixel is handled individually and is should be noted that the pixel represents the transparent colour, one disadvantage of this is that the decryption process is lossy, the area that suffers due to this is the contrast. Contrast is very important within visual cryptography because it determines the clarity of the recovered secret by the human visual system. The relative difference in the hamming weight between the representation of white and black pixels signify the loss in contrast of the recovered secret. New schemes deal with gray scale and colour images which attempt to minimize the loss in contrast by using digital half toning. Half toning allows continuous tone image, which may be made up from an infinite range of colours or gray’s to be represented as a binary image. Varying dot sizes and the distance between those dots create an optical illusion. It is this illusion which allows the human eyes to blend these dots making the halftone image appears as a continuous tone image. Due to the fact digital half toning is a lossy process in itself, it is impossible to fully reconstruct the original secret image.

All of the aforementioned studies focused on the sharing of one secret image. Due to the flexibility in practical applications and complexity in theoretical interests, the sharing of multiple secret images, in which different combinations of shares reconstruct different secrets, becomes a significant research topic. The related studies in the literature can be classified into two categories in terms of the decoding processes: (1) direct superimposition only, where the shares are stacked directly onto each other; and (2) allowing additional operation(s) before superimposition, where at least one of the shares is allowed to take one or more operations (such as flipping or rotation) before stacking onto others. Currently, the research on the first category is relatively less than the second one. Particularly, the latter has achieved the sharing of any general secrets, while the former has only involved the sharing of two secrets.

II. THRESHOLD VISUAL CRYPTOGRAPHIC SCHEME

Secret sharing is an important concept in modern cryptography. Often, it is desired that only a certain group of people can recover the secret. The concept of secret sharing was independently introduced by Shamir [7] and Blakely [7] in 1979. Secret sharing becomes indispensable whenever secret information needs to be kept collectively by a group of participants in such a way that only a qualified subgroup is able to reconstruct the secret. An example of such a scheme is a *k-out-of-n* threshold secret sharing in which there are *n* participants holding their shares of the secret and every *k* $(k \leq n)$ participants can collectively recreate the secret while any *k-1* participants cannot get any information about the secret .The need for secret sharing arises if the storage system is not reliable and secure. Secret sharing is also eminently useful if the owner of the secret does not trust any single person.

Threshold Secret Sharing Schemes

In secret sharing schemes, the number of the participants in the reconstruction phase is important for recovering the secret. Such schemes have been referred to as threshold secret sharing schemes.

The existing model for black-and-white visual cryptography schemes has been developed by Naor and Shamir. In this model, both the original secret image and the share images contain only black and white pixels. Each pixel in the original image is subdivided into a set of *m* black and white sub pixels in each of the *n* share images. The set of sub pixels can be represented by an *n* x *m* Boolean matrix S = [s_{ij}], where

Sij = 1 ⇔ the j^{th} sub pixel in the i^{th} share is black.

Sij = 0 ⇔the j^{th} sub pixel in the i^{th} share is white.

To distinguish between black and white pixels in the recovered image, we define a fixed threshold parameter *d*, where $1 \leq d \leq m$ ..*If* $H(V) \geq d$, then the sub pixels are interpreted as black, and if $H(V) \leq d - \alpha .m$, then the sub pixels are interpreted as white, where *H(V)* is the *Hamming weight* (the number of one's) of the 'or' ed *m*-vector *V*. The threshold parameter (*d*) is a numeric value for the point at which black areas are distinct from white. The *m* denotes the pixel expansion. This represents the loss of resolution from the original image to the share image, which is to be as small as possible. The parameter $\alpha > 0$ is called the relative contrast difference of the scheme. It is desirable to have a relative contrast difference as large as possible to minimize the loss of contrast in the recovered image. The value $\alpha.m$ is the contrast, which is greater than or equal to 1 and hence ensures that the black and white areas will be distinguishable.

Definition 2: A solution to the *k-out-of-n* visual cryptography scheme consists of two collections of *n x m* Boolean matrices C_0 and C_1. To share a white pixel, the dealer randomly chooses one of the matrices in C_0 and to share a black pixel, the dealer randomly chooses one of the matrices in C_1. The chosen matrix defines the colour of the *m* sub pixels in each one of the *n* transparencies. The solution is considered valid if the following three conditions are fulfilled:

1. For any S€C_0, the OR m-vector V of any *k* of the *n* rows in S satisfies $\omega_H (V) \leq d - \alpha .m$.
2. For any S∈C_1, the OR m-vector V of any *k* of the *n* rows in S satisfies $\omega_H (V) \geq d$.
3. For any subset $\{r_1, r_2, . . . , r_t\}$ of {1,2,. . .,n} with $t<k$, the two collections of *t x m* matrices obtained by restricting each *n x m* matrices in C_0 and C_1 to rows $r_1, r_2,\ldots, r_t$, are indistinguishable in the sense that they contain the same matrices with the same frequencies .For a visual cryptography scheme to be valid, these three conditions must be satisfied. The first two conditions ensure that some contrast in the scheme is maintained, and the third

condition ensures security in the scheme is maintained. The third condition states that no information can be obtained if less than *k* shares are stacked together. In other words, a matrix in $C_0 \cup C_1$, to less than *k* rows, will not be able to tell whether the matrix is from C_0 or C_1.To encrypt a white pixel of the original image, a matrix is randomly chosen from C_0 and is used to create the shares. A black pixel is encrypted by randomly choosing a matrix from C_1. At least two matrices in each collection are needed so that the dealer can randomly choose one of them. If the matrix is chosen randomly, a cryptanalyst, examining less than *k* shares, will not be able to predict the color of the pixel in the original secret image based on the pixel positions, since each matrix in the collection is equally likely to have been chosen.

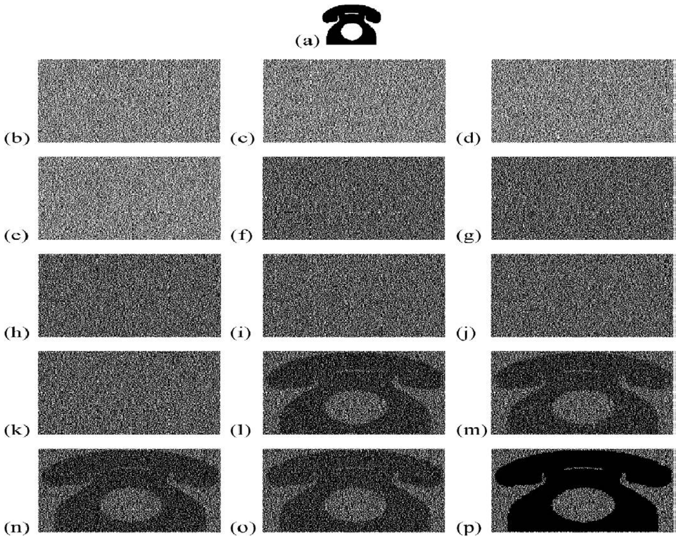


Fig. 1. Results of an implementation of Droste's (3,4) VCS:(b)S_1 ; (c)S_2,(d)S_3 ,(e)S_4 , (f)$s_1 \otimes S_2$,(g) $S_1 \otimes S_3$,(h) $S_1 \otimes S_4$, (i) $S_2 \otimes S_3$, (j) $S_2 \otimes S_4$,(k) $S_3 \otimes S_4$, (l) $S_1 \otimes S_2 \otimes S_3$, (m) $S_2 \otimes S_4$, (n) $S_1 \otimes S_3 \otimes S_4$, (o) $S_2 \otimes S_3 \otimes S_4$, and (p) $S_1 \otimes S_2 \otimes S_3 \otimes S_4$.

III. THRESHOLD MULTIPLE-SECRET VISUAL CRYPTOGRAPHIC SCHEME

A conventional (k, n)-VCS shares one secret image among n participants following the (k,n) access structure. Here, we consider the sharing of multiple, say, secret images among participants.

3.1 Problem Specification of (k, n,s)-MVCS

Essentially, a (k,n,s) MVCS [25] is capable of encoding secret Images P1,P2,P3…..Ps into shares S1,S2,…Sn which are distributed to the participant in P={1,2…..n} such that each group of k,k+1,….,n shares reveals P1,P2,P3…..Ps respectively, to our eyes when superimposed, but that of less than shares cannot. Here, s=n-k+1 and the cases of s $\leq$n-k+1 can also be generated.

Definition 1:

To reveal (or conceal) one pixel ,p P, either white (0) or black (1) with only two possibilities, in the superimposed result of k (or less than k) shares, the (k,n)-VCS aims at the design of a set of two basis matrices B^0 and B^1 for encoding P=0 or 1, respectively. Now, a set of corresponding pixels (p1,p2…ps) , either 0 or 1 for each with totally 2^s possibilities, should be considered in a (k,n,s) -MVCS where pixels ,p1 $\in P1, p2 \in P2$,..ps Ps are regarded as corresponding to each other if their positions in the secret images are all the same. To reveal (or conceal) these corresponding pixels (p1,p2…ps) in the superimposed results of k.k+1,…..n(or less than) shares, respectively, the (k,n,s)-MVCS should rely on a set of nXm 2^s basis matrices $B^{00..0}$,$B^{00..1}$, $B11^{..1}$ to encode (p1,p2…ps) =(0,0,..0),(0,0,…1),…,(1,1,…1),respectively, into m sub pixels for each of the n shares. Assume U={i1,i2….i_u} and V={j1,j2….jv} Where U,V € {1,2…n}, and 1. Let $B^{(p1,p2…ps)}[U]$ ($B^{(p1,p2…ps)}[V]$) denote the $u^{\times m(v \times m)}$matrix consists of rows i1,i2….i_u {j1,j2….jv} in $B^{(p1,p2…ps)}$

Definition 2:

A set of 2_S Boolean basis matrices $B^{0..00}$,$B^{0..01}$..,$B^{1\ldots 11}$, in which the result of a column permutation of $B^{(p1,p2\ldots ps)}$ defines the color of the m sub pixels in each one of the shares when sharing corresponding pixels (p1,p2…ps) $\in \{0,1\}$ in p1,p2…ps, respectively, constitutes a (k,n,s)-MVCS where s=n-k+1 if the following conditions are met:

1) For each set of t+(k-1) participants U € P where 1<T<S And k<|U|(=t+(k-1))<n ,

2) For each set of less than k participants V€ P(1≤|v|≤ for K-1),H($B_V^{P1,P2,\ldots..PS}$)=H($B_V^{P1',P2'\ldots\ldots\ldots\ldots PS'}$),for p1,p2…ps $\neq p1',p2',\ldots\ldots..ps'$ where pi,pj' € {0,1} and 1≤ i ,j≤s.

3.2 HALFTONE VISUAL CRYPTOGRAPHY:

Halftone is the reprographic technique that simulates continuous tone imagery through the use of dots, varying either in size or in spacing, thus generating a gradient like effect. "Halftone" can also be used to refer specifically to the image that is produced by this process.

Where continuous tone imagery contains an infinite range of colours or greys, the halftone process reduces visual reproductions to an image that is printed with only one color of ink, in dots of differing size or spacing. This reproduction relies on a basic optical illusion. Optical illusion means the tiny halftone dots are blended into smooth tones by the human eye

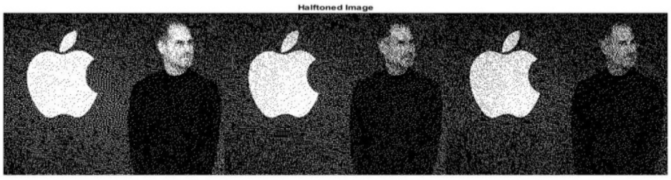


Fig 2: Half tone image

3.3 REVERSE VISUAL CRYPTOGRAPHY:

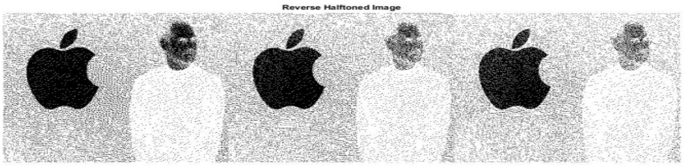
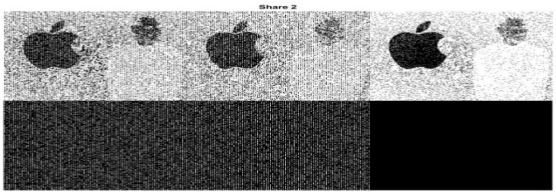


Fig 3: reverse halftone image

It is exactly opposite to the original halftone image ,it covets white dots into black and black into white.

3.4 GENERATION OF SHARES:

From the above halftone and reverse halftone images this concept can generate the shares which is shown below



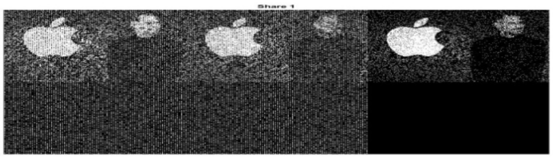


Fig 4 : generation of shares

3.5 SUPERIMPOSITION OF SHARES :

Using bit or operation between shares we get superimposed output:

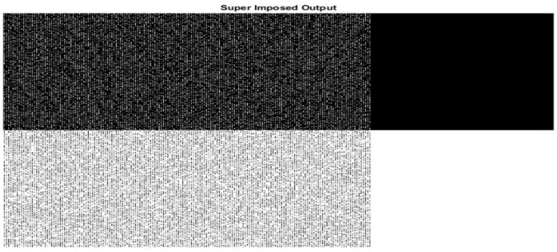


Fig 5: super imposed output

3.5 BLOCK DIAGRAM:

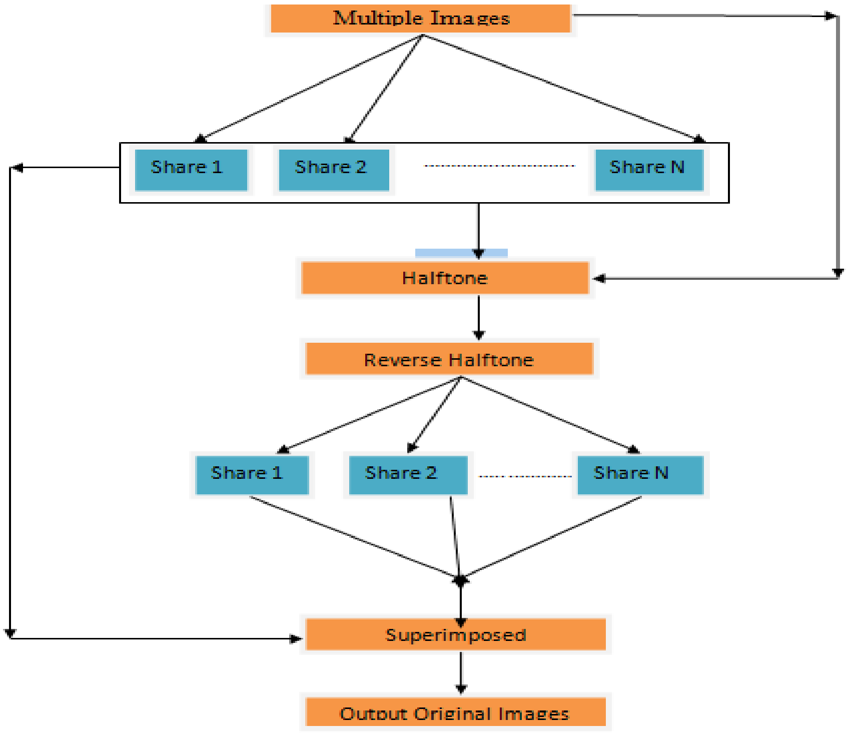


Fig 6: block diagram

From above image can be divided into 3 shares from that we generate halftone image which represents white and black dots and generate reverse halftone image which is exactly opposite to the halftone images which convert white into black and black into white. From the halftone and reverse halftone images, generate shares. Generated shares can be superimposed by using BIT OR operation and obtain superimposed output.

IV. CONCLUSION

We give formal definitions to threshold multiple-secret visual cryptographic schemes, namely (k,n,s) -MVCS and (k,n,s,R)-MVCS, using only superimposition without any additional operation in decoding process. General constructions for both schemes are designed using the skills of linear programming in which the objective functions are to minimize the pixel expansions with the constraints satisfying the revealing, concealing and security conditions in the corresponding definition. The minimum pixel expansions obtained by for both schemes under different problem scales are summarized and reported, which have never been discussed before in the literature.

The proposed definitions are innovative and significant in revealing there search of visual multiple-secret sharing using only superimposition. The design of the integer linear programs for (k,n,s) -MVCS and (k,n,s,R)-MVCS is novel and flexible to be applied to various types of VCSs.

Even though the proposed constructions are focused on binary secret images, they are applicable to color secret images by exploiting the skills of half toning, color decomposition, color combination, and so on [15]. It is noticed that the pixel expansion reported are of theoretical interest, yet, some of them, especially when or grows larger, lose the practicability due to the large pixel expansion and degraded contrast. We would not suggest applying the proposed MVCSs for such cases inpractical applications.

Thus, we may utilize their findings to work on the topic of maximizing contrast in visual multiple-secret sharing.Further,as pointed out,for agiven setting of k,n and s, “which revealing list may produce the smallest pixel expansion” and “how does a revealing list affect the resultant pixel expansion” are challenging topics worthy of further investigation.

REFERENCES

[1] G. Ateniese, C. Blundo, A. De. Santis, and D. R. Stinson, “Extende capabilities for visual cryptography,” *Theoretical Computer Sci.*, vol.250, pp. 143–161, 2001.

[2] G. Ateniese, C. Blundo, A. De. Santis, and D. R. Stinson, “Visual cryptography for general access structures,” *Inf.Computat.*, vol. 129, pp.86–106, 1996.

[3] G. Ateniese, C. Blundo, A. De. Santis, and D. R. Stinson, “Constructions and bounds for visual cryptography,” *Lecture Notes Computer Sci.*, vol. 1099, pp. 416–428, and 1996.

[4] G. R. Blakely, “Safeguarding cryptographic keys,” in *Proc. Nat. Computer Conf.*, 1979, vol. 48, pp. 313–317.

[5] C. Blundo, A. De. Santis, and D. R. Stinson, “On the contrast in visual cryptography,” *J. Cryptology*, vol. 12, pp. 261–289, 1999.

[6] C. Blundo, P. D’Arco, A. De. Santis, and D. R. Stinson, “Contrast optimal threshold visual cryptography schemes,” *SIAM J. DiscreteMath.*, vol. 16, pp. 224–261, 2003.

[7] C. Blundo, S. Cimato, and A. De Santis, “Visual cryptography schemes with optimal pixel expansion,” *Theoretical Computer Sci.*, vol. 369, pp.169–182, 2006.

BIOGRAPHY

Smt.V.Chinnapu Devi has pursued her B.E from SLN College of engineering, Raichur and MTech from G.Pullareddy college of engineering, Kurnool. Presently she is working as Associate Professor in Brindavan Institute of Technology & Science, Kurnool. She has published 4 International Journals. Her research areas of interest are Digital image processing and communication.

S.Nikitha is pursuing her B.Tech in Electronics and communication engineering from Brindavan Institute of Technology & science, Kurnool.

M.Mahesh is pursuing her B.Tech in Electronics and communication engineering from Brindavan Institute of Technology & science, Kurnool

.

Shaik.Moulali is pursuing her B.Tech in Electronics and communication engineering from Brindavan Institute of Technology & science, Kurnool

.