International Journal of Latest Trends in Engineering and Technology
Vol.(9)Issue(4), pp.045-051
DOI: http://dx.doi.org/10.21172/1.94.08
e-ISSN:2278-621X

MULTI – PIXEL PRVC ENCODING SCHEME USING DYNAMIC ACCESS CONTROL CONSTRUCTION IN VISUAL CRYPTOGRAPHY

Ch.Ratna Babu[1] & Dr. B.Raveendra Babu[2]

Abstract: Visual Secret Sharing (VSS) techniques are introduced to manage visual information security in the visual cyber world. Visual secret sharing schemes are new visual cryptographic systems, which allows secret sharing information to be encoded in such a way that deciphering can be achieved through the human visual system (HVS), without using the computer. Single pixel encoding method in which only one pixel can be encrypted at each encoding run. But the encoding efficiency is very low for such methods. Multi-pixel encoding is an evolving scheme in visual cryptography for that it can scramble more than one pixel for each scrambling run. It takes the secret image and perceives a pixel chunk with as many pixels as possible to encrypt for each run. A pixel chunk comprises of consecutive pixels of same type for the encrypting. The proposed scheme brings advantage for the encoding efficiency over single pixel encoding and other known multi-pixel encoding methods. This paper presents a novel multi-pixel encoding scheme using access control structure. Furthermore, this scheme can work very well for general access structure and also for gray-scale images without pixel expansion. The outputs of this scheme establish that it can achieve good quality for overlapped images.
Keywords: Shares, Secret Sharing, Pixel expansion, Threshold, Access control structure, DACC, PRVC.

1.INTRODUCTION

With the rapid advancement of visual cyber world, visual multimedia information is transmitted over the Internet. Different confidential visual cyber data such as military maps, financial and commercial identifications are transmitted over the Internet. While using visual secret images, security issues should be taken into consideration because intruders may utilize weaknesses over communication to steal information that they want. To deal with the security problems of secret images, various image secret sharing schemes have been evolved.

Visual Cryptography (VC) is the study of mathematical techniques related aspects of visual information security such as confidentiality, data security, and data origin authentication. Visual cryptography proposed by the Naor and Shamir [1], is a technique for protecting secret image shares that has a computation – free decryption process. In basic Naor and Shamir method, each information image is separated into two shares so that no information can be reconstructed from any single share. Each share is printed in transparancies.The decryption is made by heaping the two transparencies and the evidence image can be revealed without using any complex computations. For instance, a security guard checking the worker ID or a secret mediator improves an urgent secret at some place where no electronic gadgets are applied. In that conditions, the HVS is one of the most convenient way and are reliable tools to do checking and secret recovery. The intent of this paper is to provide an overview of VSS techniques and which précises the works study in VC and its extensions.

2. RELATED WORK

2.1. Basic (2x2) VC Scheme

Fundamental (2x2) VC scheme enrooted by the Naor and Shamir [1], that takes input gray image 'B' as information and it is further split 'n' into no of transparencies. Each picture element 'p' of gray image 'B' is scrambled into two transparencies and each transparency contain the expanded pixels. In this model gray image or message is a collection of white and black pixels, each white pixel is represented by the transparent color, and each black pixel represented by the information. The fig.1 shows the superposition of the share1 and share2 to get the revealed message or decrypted image as a result. No information can be reconstructed using single share and each share is printed in transparencies.

[1] Research Scholar, Acharya Nagarjuna University, India
[2] Professor, Dept. of CSE, RVR & JC College of Engineering, Guntur, India

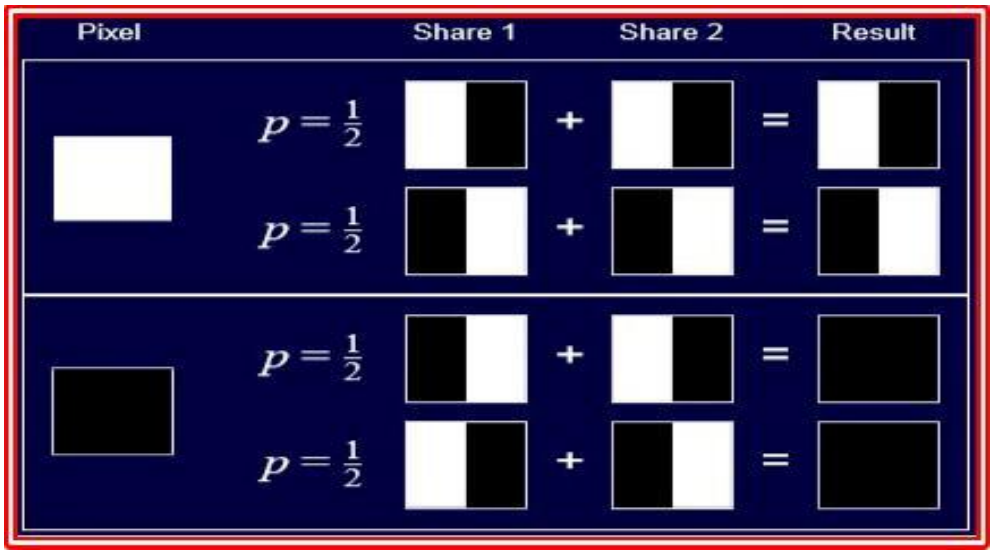


Fig. 1 Basic (2x2) VC Scheme

Finally the each share loss the contrast in the revealed image. The fig.2 shows the results of the basic (2x2) VC scheme and it is implemented in java language using java image frame work.

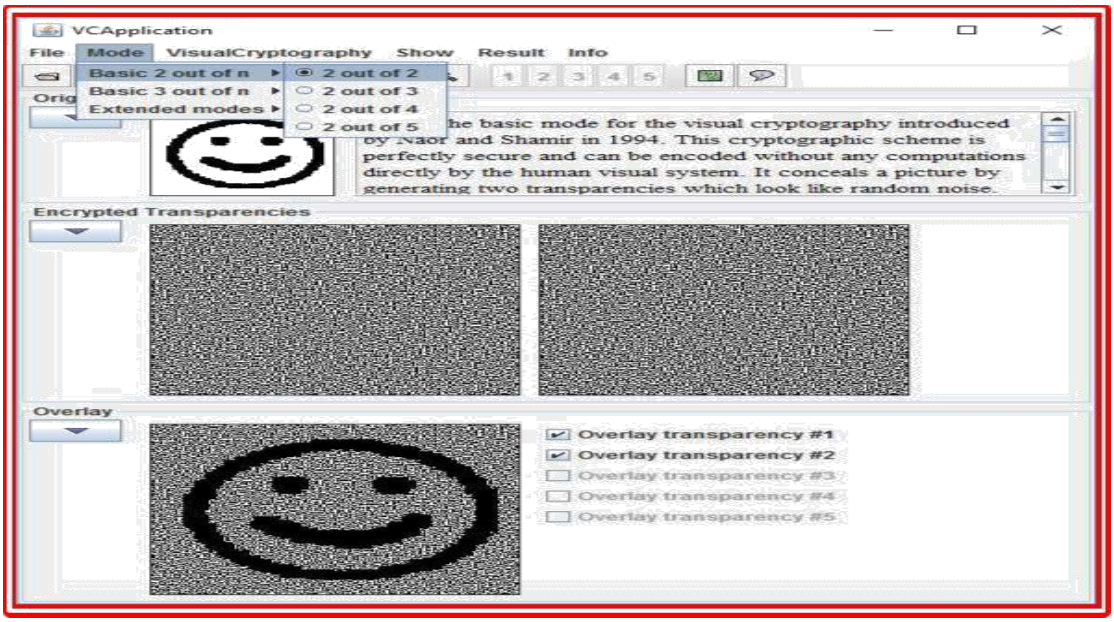


Fig.2 Basic Naor and Shamir Result

2.2. Extended (k, n) VC for Natural Images

The basic (2x2) VC Scheme was extended into the threshold VC model in which 'k' is the reveal shares in the secret image. The basic difference between (2x2) VC scheme and threshold VC scheme is only one that is in (2x2) VC model, the threshold value is 'n' whereas in threshold VC scheme 'k' is a subset of 'n'. Each pixel either black or white of gray image [5] 'B' appears in 'n' shares and each share is divided into 'm' sub-pixels. One pixel is represented by 'n x m' Boolean adjacency matrix Z = [cij], cij = 1 iff j^{th} sub-pixel in the i^{th}

share is black. For example 2 out of 2 scheme with 2 sub pixels such as White pixels: $\begin{matrix}0 & 1 & 1 & 0\\ 0 & 1 & 1 & 0\end{matrix}$,

Black pixels: $\begin{matrix}1 & 0 & 0 & 1\\ 0 & 1 & 1 & 0\end{matrix}$, Similarly the results of k out of m scheme shown in the fig.3.

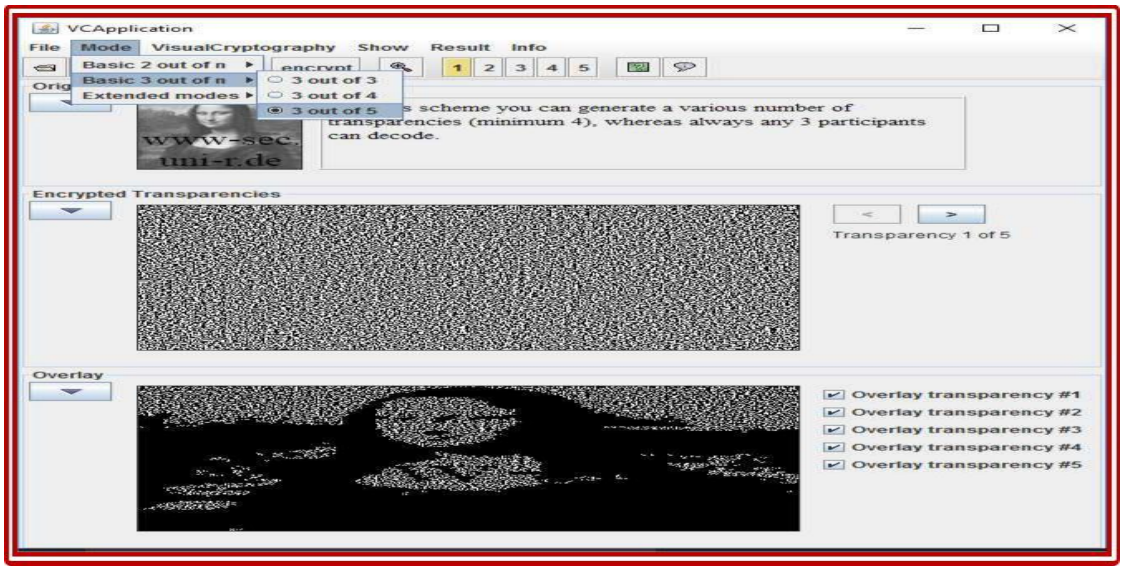


Fig 3. (3, 5) threshold VC Scheme where k=4

2.3. Recursive Threshold VC Model

The k x n threshold VC model discussed in above section uses 'k' transparencies to reveled the secret image. Each share consists at most [1/k] bits of secrets. This scheme also suffers from ineffectiveness in terms of number of bits of stealthy conveyed bit of shares. Recursive threshold VC scheme defined by Abhishek Parakh and Subhash Kak [2] eliminates this problem by hiding smaller secrets in shares of larger secrets with secret sizes doubling at every step. In this approach also, the security is lost when pixels are expanded.

2.4 Regional Incrementing for VC Models

Usually above VC techniques are at a time use all of the pixels in the secret image are revealed and shared using a single rule. This type of sharing policy reveals either the entire image or nothing, and hence limits the secrets in an image to have the same secrecy property. Ran-Zan Wang [7] proposed the Region Incrementing Visual cryptography (RIVC) for sharing visual secrets in multiple secrecy levels in a single image. In the 'n' level RIVC scheme, an image S is designated to multiple regions associated with secret levels, and encoded to shares with the following features:

(a) Each share cannot obtain any of the secrets in S,
(b) Any t ($2<t<n+1$) shares can be used to reveal (t-1) levels of secrets
(c) the number and locations of not-yet revealed secrets are unknown to users,
(d) all secrets in S can be disclosed when all of the (n+1) shares are available

2.5. Segment Based VC

All the above VC techniques are based on working pixels. The drawback of pixel based visual cryptography is the loss in contrast of the reconstructed image which is directly proportional to pixel expansion 'm'. The approach proposed by Bernd Borchert [8] is based on segments which take pixels as the small segments to be encrypted. The advantage of segment based over pixel is that it may be easier for the human eye to recognize the symbols, the messages consist of numbers which can be encoded by segment based visual cryptography using seven segment display. This approach violates the security whenever the size of the message increases and it works only for some set of encoded symbols.

2.6 PRVC Algorithm for VC Model

In Pseudo – Randomized Visual Cryptography model, decoded image and original secret message are of same size since there is no pixel expansion effort. Hiding of the visual information based on pseudo randomization is proposed by Ch.Ratna Babu, M.Sridhar, and B.Raveendra Babu [10]. The PRVC method revealed good confidentiality due to its randomness and also some visual impairments are encountered due to reduce its size . The secret decoded image is darker than the original and increases the spatial resolution by using pixel reversal [11]. The visual cryptography has the same effect in the decoded image .In this approach, no pixel expansion happens but the security is average.

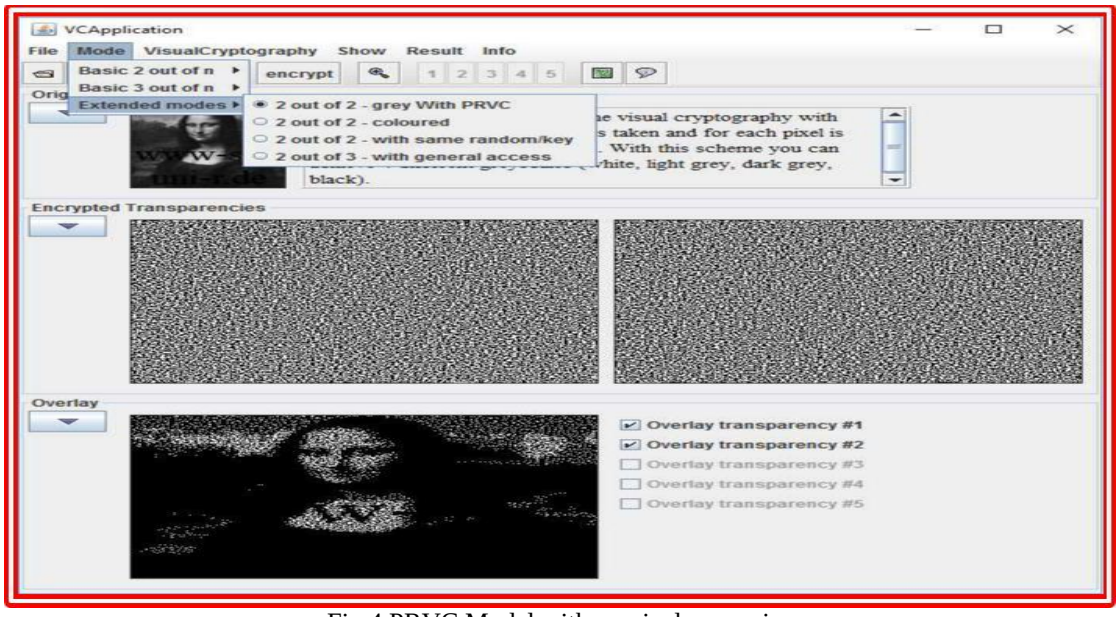


Fig 4.PRVC Model with no pixel expansion

3. PARAMETERS OF VSS SCHEMES

Naor and Shamir [1] suggested two main parameters, expansion factor‘t’ and contrast ‘α’:

a) Expansion Factor ‘t’, is the No of transparencies used to encipher the secret image. Expansion Factor‘t’ increases the decrease the quality of the revealed image resolution.

b) Contrast Factor ‘α’, is the difference between two pixels in the revealed image. Hence contrast factor is the quality of the revealed image. If Contrast Factor is smaller then security is loss in the reconstructed image.

Jung-San Lee et al [12] proposed privacy, expansion factor, quality and time complexity. Security is satisfied if each share reveals no information of the original image and the original image cannot be reconstructed if there are fewer than k shares collected.In every VC Scheme k, there is a k out of k scheme with $m = 2^{k-1}$, $a = 1/2^{k-1}$, $r = 2^{k-1}!$ .Construct k x 2^{k-1} matrices, M^0 (white pixels) and M^1 (black pixels) as:

M^0 contains the 2^{k-1} vectors with even number of 1’s M^1 contains the 2^{k-1} vectors with odd number of 1’s

P0 and P1 consist of all permutations of columns in M^0 and $M^{1.}$ Naor and Shamir suggested any k out of k scheme such that $\alpha \leq 1/2^{k-1}$ and $m \geq 2^{k-1}$.

4. PROPOSED SCHEME

In single pixel encoding method single pixel can be enciphered each stage of encryption layer and its encoding complexity too low. In 2004, Hou et al. [13] enrooted a multi-pixel enciphering scheme in which at each iteration ‘m’ array of pixels used in enciphering, where ‘m’ is a pixel expansion factor. (2x2) VC access structure schemes exhibits poor quality for the revealed constructed image .Later, Y. C. Hou and S. F. Tu, [14] proposed another multi-pixel encoding scheme to improve the quality of revealed image, but it also encodes ‘m’ pixels at each iteration nevertheless the ‘m’ pixels are of same type. The main drawback in this scheme is ‘m’ consecutive pixels of same type used in the next iteration .Finally redundant pixels information encountered for the next iteration.

4.1 Dynamic Access Control Construction (DACC)

DACC is a rule that define how to share a secret information and rule is created during runtime. In (k,n) DACC method generate rules that any ‘k’ or more out of ‘n’ transparencies can cooperate to reveal the secret image and any less than ‘k’ transparencies together get nothing about the secret image. Generally (k x n) threshold access structure loads all transparencies to cooperate for a secret recovery and therefore nothing can be reveal even if one transparency is absent. It is easy to know that a (t, n) threshold access structure is tolerant because the final secret still can be restored from the other k transparencies when up to (n – k) shares are corrupted even.

Generally the basis matrices C0 and C1 are represents white and black pixels and these are used encoding process. C0 and C1 are the same dimension n × m. Suppose the secret image is GI with t1 × t2 pixels and the n transparencies are p1, p2,,…, pn, respectively. In gray-scale images, the white pixel usually means blank and black pixel means non-blank. However, (k x n) threshold access structure is only one special case of the so-called dynamic access control structure. Usually, access control structure is denoted as set of transparencies P={p1,p2,p3,..pn} , T = { CQual, CForb} where CQual and CForb are sets of subsets of all transparencies and if CQual

∩ CForb=⌀ then (CQual,CForb) is general access control structure .Here CForb denotes a collection of prohibited or Forbidden sets and CQual denotes a collection of qualified sets. It is easily known that overlaying all the transparencies held

by the users of any qualified set can recover the secret image but stacking all the shares held by the participants of any forbidden set cannot reveal information about the secret image. For example, in a system with 3 participants, let CQual = {{p1, p2}, {p1, p3}, {p1, p2, p3}} which implies that CForb = {{p1}, {p2}, {p3}, {p2, p3}}. Therefore, overlaying share p1 and share p2 can reveal the secret image; however, overlaying share p2 and share p3 can reveal nothing about the secret image.

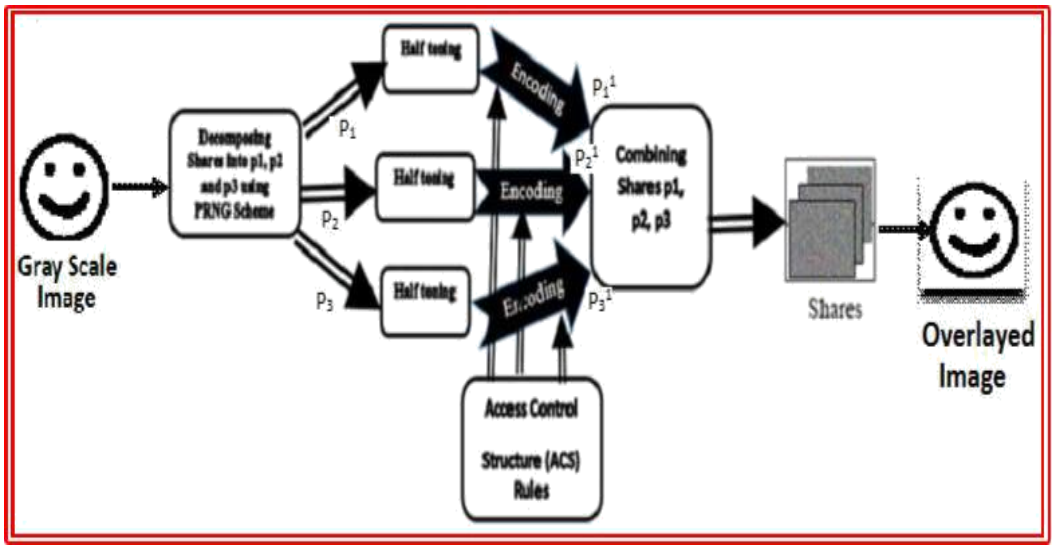


Fig .5 Multi – Pixel Encoding PRVC Scheme using DACC

4.2. Algorithm: Multi – Pixel Encoding PRVC Scheme with DACS

Input: Gray- Scale Image (GI) with t1 × t2 pixels size, basis matrices C0 and C1 with size of n × m, respectively.

Output: The shares p1, p2,…, pn each with t1 × t2 pixels, respectively.

Method:Step1: Generate the Secret Shares P={p1,p2,..pn} using PRVC Model [10] until meeting different pixel or reaching the end of GI,

Step 2: DACS=∅; Select the Qualified subset (CQual) of shares and it is CQual C 2^P

Step 3: Identify the collection of forbidden sets (CForb) of shares and it is CForb C 2^P

Step 4: if CQual ∩ CForb=∅ then DACS = (CQual,CForb).

Step 5: this process will be repeated until the new access control rule is generated.

Using the above algorithm, take each gray-scale image whose intensity ranges from zero to 255. It can transform each gray-scale image into a binary image by half toning. Then each half toned image can be encrypted by the proposed scheme under the control of an appointed access structure. Finally, the three encrypted transparency images are again combined to form an intact share. While constructing, one need to stack all the legal shares to reveal the secret image. The whole encryption procedure of the proposed scheme for gray – scale images code snippet for Multi – Pixel Encoding PRVC Scheme with DACC is illustrated in Fig. 5. The following java pseudo code snippet to discuss the Multi – Pixel Encoding PRVC Scheme with DACC.

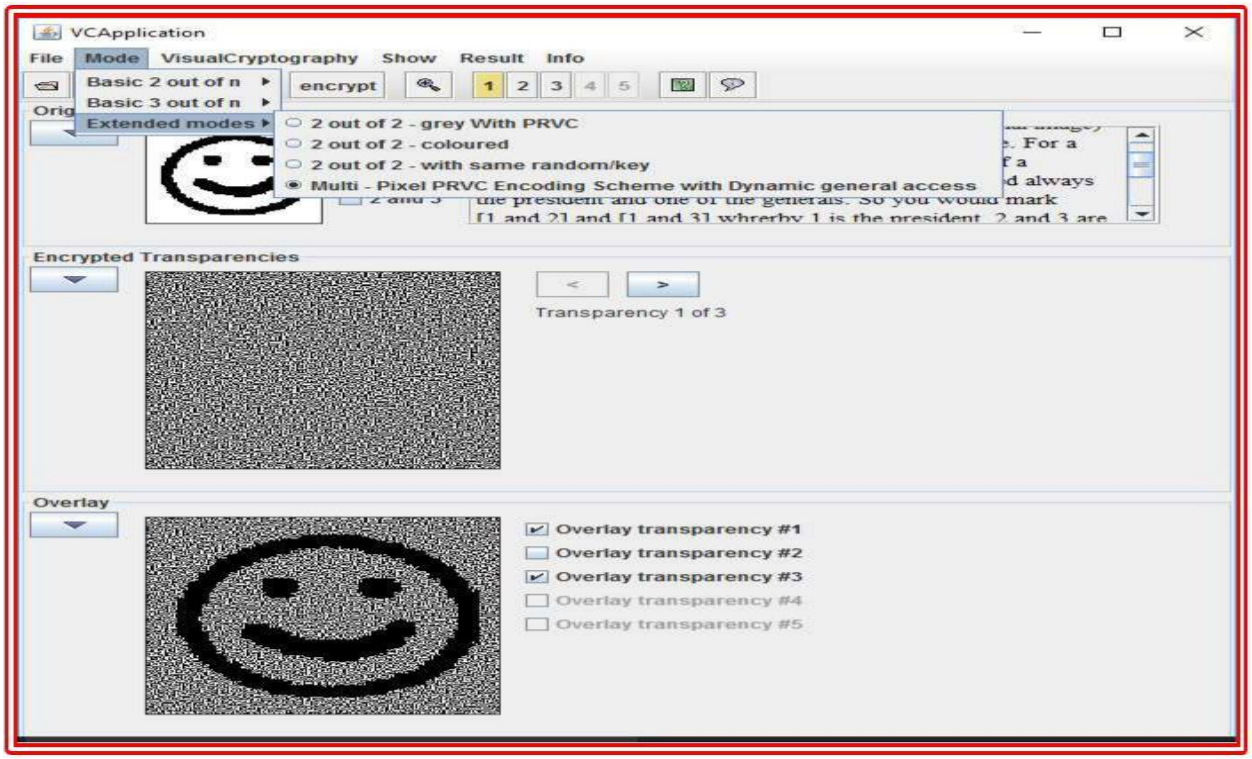
4.3. Pseudo Code Snippet: Multi – Pixel Encoding PRVC Scheme with DACC public class EncDACC extends Encryptor {

```
/** store the encryptor to get some of the init-matrices*/ private Encryptor m_enc = null;
/** store the access structure for this scheme*/
private boolean[] m_structure;
public EncDACC(boolean[] ga, int height, int width, int n){
```

```
super(height, width, n);
System.out.println("Encryptor with DACC");
if(ga[0]&&ga[1]&&ga[2]){
m_enc = new Enc2_n(width, height,3);
m_initMatrixC0 = m_enc.getInitMatrixC0();
m_initMatrixC1 = m_enc.getInitMatrixC1();
} else if((!ga[0])&&(!ga[1])&&(!ga[2])){
m_enc = new Enc3_3(width, height,3);
m_initMatrixC0 = m_enc.getInitMatrixC0();
m_initMatrixC1 = m_enc.getInitMatrixC1();
} else {
m_enc = new Enc2_2(width, height,2);
m_structure = ga;
m_initMatrixC0 = new IntMatrix(3,4);
m_initMatrixC1 = new IntMatrix(3,4);
this.setupStartMatrix(this.getDACCMatrix());
}
}
/** sets up the encryptor object with a new access structure
public EncDACC getEncDACCWithNewAccessStructure(boolean [] ga, Image newImage){ EncGA instance = new EncGA(ga,m_wSrc, m_hSrc, 3); instance.initEncrypt(newImage);
instance.encrypt();
return instance;
}
```

5. EXPERIMENTATION RESULTS

The Multi – pixel PRVC encoding scheme is implemented in Java technology using Net Beans IDE environment. Experimentation results of the algorithm is shown in fig. 6 using dynamic general access construction T = {CQual, CForb} and it is stacked images are of better visual quality.



.Fig 6. Multi – Pixel Encoding PRVC Scheme with DACC

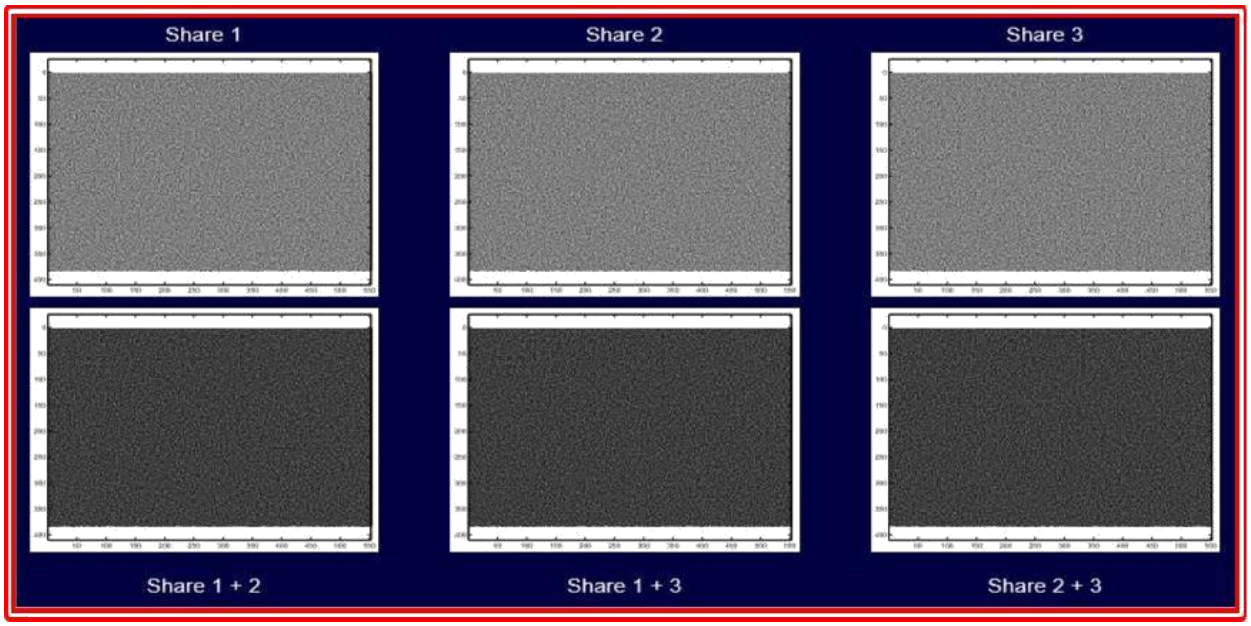


Fig 7. Multi – Pixel Encoding PRVC Scheme with DACC iterations

6. CONCLUSION

In this paper different visual cryptography schemes are studied and their working process is evaluated based on number of secret shares, pixel expansions and security. Also a novel Multi-pixel PRVC encoding scheme is suggested in this paper using dynamic access control structure. From the experimental results, it works well for grey-scale images or Halftone images. Multi-pixel PRVC scheme produce the better quality for stacked images and high efficiency for encoding in secret sharing. These advantages are very useful for business application in cyber world for information security.

7. REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography, " Advances in Cryptology-Eurocrypt'94, pp. l–12, 1995.
[2] Abhishek Parakh, Subhash Kak: A Recursive Threshold Visual Cryptography Scheme CoRR abs/0902.2487: (2009).
[3] Chang-Chou Lin , Wen-Hsiang Tsai, Visual cryptography for gray-level images by dithering techniques, Pattern Recognition Letters, v.24 n.1-3.
[4] G. Ateniese, C. Blundo, A. DeSantis, D.R. Stinson, Visual cryptography for general access structures, Proc.ICALP96,Springer,Berlin,1996, pp.416-428.
[5] Nakajima, M. and Yamaguchi, Y., Extended visual cryptography for natural images. Journal of WSCG. v10 i2. 303-310.
[6] Jin, D., Yan, W. and Kankanhalli, M.S., Progressive color visual cryptography. J. Electron. Imaging. v14 i3.
[7] Wang, R.Z.[Ran-Zan], Region Incrementing Visual Cryptography, SPLetters(16), No. 8, August 2009, pp. 659-662.
[8] Bernd Borchert, Klaus Reinhardt: Abh or- und manipulation ssichere Verschl usselung f ur Online Accounts. Patent application DE-102007-018802.3, 2007.
[9] HU Chih-Ming, TZENG Wen-Guey, "Cheating prevention in visual cryptography", IEEE transactions on image processing ISSN 1057-7149 ,2007, vol. 16, no1, pp. 36-45.
[10] Ch.RatnaBabu, M.Sridhar and Dr.B. RaveendraBabu, Information hiding in gray scale images using pseudo-randomized visual cryptography algorithm for visual information security, Proceedings of IEEE International Conference on Information Systems and Computer Networks (ISCON), at Gala University, Matura, ISBN:978-1-4673-5987-0, 9-10 March 2013, pp.195 – 199.
[11] Ch.RatnaBabu, M.Sridhar, and Dr.B. RaveendraBabu, Improved PRVC Algorithm for Halftone – Images, Proceedings of Elsevier National Conference on Emerging Trends In Information technology
[12] Jung-San Lee, T. Hoang Ngan Le, Hybrid (2, N) Visual Secret Sharing Scheme For Color Images, 978-14244-4568-4/09, IEEE, 2009.
[13] Y. C. Hou and S. F. Tu, "Visual cryptography techniques for color images without pixel expansion,"
[14] Y. C. Hou and S. F. Tu, "A visual cryptographic technique for chromatic images using multi-pixel encoding method," Journal of Research and Practice in Information Technology, vol. 37, no. 2, pp. 179–191, 2005.