

Seeable visual but not sure of it - A visual cryptographic perspective for TAMIL characters

Rengarajan Amirtharajan^{#1}, Sumaiya Sulthana^{*2}, P. Shanmuga Priya^{#3}, G. Revathi^{#4}, A. Kingsly Infant^{#5} and J.B.B. Rayappan^{#6}

[#] School of Electrical & Electronics Engineering, SASTRA University, India- 613401.

¹amir@ece.sastra.edu, ²sumaiya.ullah@gmail.com, ³shanpri.g@gmail.com, ⁴gg.revathi.7@gmail.com,
⁵kingslyinfant09@gmail.com, ⁶rjbosco@ece.sastra.edu

Abstract— In this paper apprized three paradigms for visual cryptography for TAMIL Characters, wherein k out of n shares is sufficient to see the confidential information. Visual and polynomial-based are the two major categories in cryptography. This paper incorporates both simple and composite models to accomplish secret sharing. Secret data is sent to the holders as shares but how they decrypt the shares to retrieve the secret is a closed book. Procedures involved in sectoring the secret as shares need to be very intricate enough to attack. Advantages of visual cryptography are no requirement of cover image, unable to recovery with partial shares, litheness, and ease of sending each share in different media and so on. This paper suggests three such methods wherein the shares submit themselves to unequaled manipulative processes and then sent to the holders. For readers all the inputs, their shares and the decrypted output are depicted for better understanding without decryption.

Keyword- Information security, Visual Cryptography, (k,n) Shamir VC, Share rotations, Pixel rotation.

I. INTRODUCTION

Cryptography is an ancient art of hiding clandestine message and it intended for one to one communication. Its electronic version is now being extensively used in secret sharing schemes with updating in its own right. Its classification can be stated as symmetric, asymmetric, trust models and hash functions. Main aim of cryptography is protection of data [1]; here data to be safeguarded is termed as plain text, modified version of plain text is nothing but cipher text. The attack performed on cryptography is known as Cryptanalysis. The term visual cryptography signifies sheltering secrets in or as images [2]. The secret is sometimes visible but not always where the main concern is detectability. Secret sharing schemes involving cryptography and images (Steganography) have become a new field of interest and have gained popularity among scholars in diverse fields.

Visual cryptography plots are expansively inspected right from their contraption and now are pulled out to copious appliances like ocular endorsement and credentials, encryption and steganography. Challenge posed in this type of cryptographic arena is fictitious lucidities and its management. Having mentioned this, it is also noteworthy that many deceitful bars have also been in action. Use of manifold covert images and generic algorithms may help for counteraction. Even though, furtive sharing and VC look alike, there are some distinctive properties exist between them. To cite some, extracted image may have slight distortion, recovery process need not involve cryptographic calculation, no need of cryptographic familiarity. A common term one can come across in VC is 'share' which may also be labelled as transparency [3-5].

Studies in visual cryptography mainly concentrate in image quality and reducing pixel expansion [6-8]. Different types of visual cryptographic schemes are of gray, chromatic, specific-feature, extended and XOR-based [10-13]. Since in general, most VCSs share a single secret, only limited applications are able to be developed [2-13]. To overcome this, multi-secret sharing proposals are later built up [9]. The fundamental principle depends on shadows which can be rotated, stacked, circularly shifted or ringed. Last two types can infix secret images in unlike angles more willingly than explicit ones in rectangular shades.

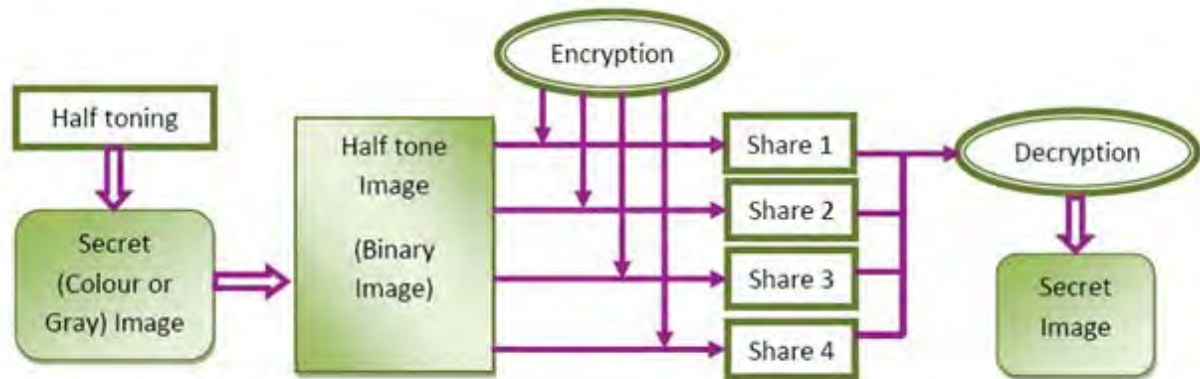
VCS is one of its kind image secret sharing schemes where secrets are shared and are themselves images. It just encrypts the image into transparencies that contain the shares which are to be distributed to the participants [10-13]. Investigators pay attention to contrast and pixel expansion where the latter defines the amount of sub pixels needed to encode every pixel which is to be a minimum value whereas the former detects the differences between black and white pixels in an image that is reconstructed. VCSs are now being adoptive in various applications like image indexing, safe and sound display, watermarking and engrafting confidential message. Currently, various combinations produce better outcomes in visual cryptography rather than sticking to one.

In this paper, Section II explains three visual cryptographic methods for tamil secret and its results are discussed followed by conclusion in section III.

II. PROPOSED METHODOLOGY

A. Method 1- (k, n) – Threshold Scheme

The basic block diagram for visual cryptography is shown in Fig. 1. Here, input secret image may be colour or gray scale image. If it is colour image, it should be converted into gray scale image to make encryption easy. Then secret image is converted into binary image using halftoning which is nothing but dithering. Binary image consists of only black (0) and white (1) pixels.

Fig. 1. Block diagram for (k, n) - Threshold scheme

Encryption is performed on binary image to produce shares. First encryption function is applied on binary pixels of secret image to create various shares (S_1, S_2) which contains $m_1 \times m_2$ (2×2) sized blocks.

For n shares, there are $n \times m_1 m_2$ basis matrices.

For n users, there are $n(n \times m_1 m_2)$ basis matrices.

Lookup table for this method is presented in table 1. Each pixel in S_1 and S_2 shares are equivalent to each other if the secret pixel is white (1) which can be represented by variable C_1 . If the secret pixel is black (0), then each pixel in shares S_1 and S_2 are complement to each other and it can be represented by variable C_0 . After that, decryption is happened by stacking process which is applied on shares to produce original secret image.

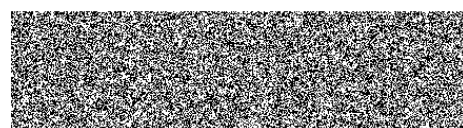
TABLE I
Lookup table for (k, n) – Threshold Scheme

Pixel	□						■					
Share 1	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□
Share 2	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□
Stack	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□

Sample results for this method with four shares are shown in Fig. 2. Here input image is divided into four shares and then combined to get output image.

சாஸ்த்ரா

Input



Share 1

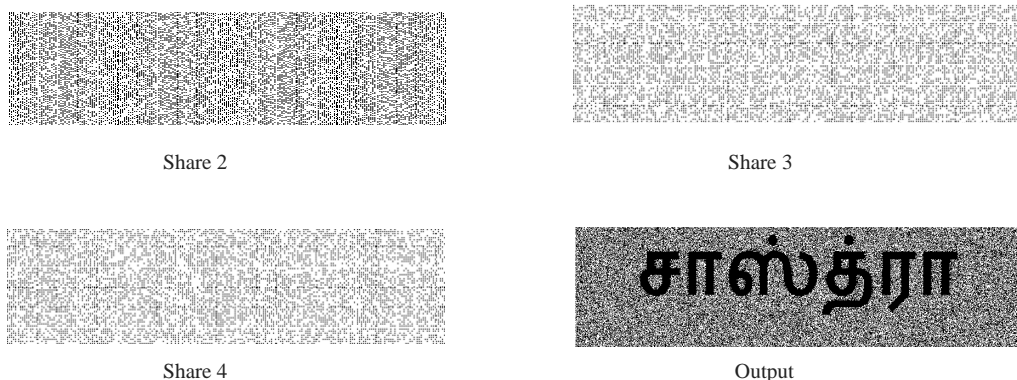


Fig. 2. A sample result for (k, n) threshold scheme – Tamil writings

B. Method 2- Pixel Rotation

Sharing of two images is discussed here. Only two shares (S_1 and S_2) are created for two secret images. The shares must be of same size and probably it is of square shape here, since this superimposition in different means creates the secret image. Individually the shares S_1 and S_2 cannot tell anything about secret image. This proves the security of this algorithm.

Rotation of share is involved here to increase the complexity. Here the first share S_1 can be rotated by an angle of θ say 90° , 180° or 270° . In this method, Share1 is rotated by 270° and then stacked with share2 for getting the secret image 2. Secret image 1 can be obtained by stacking share1 and share2 together.

Lookup table for generating share blocks in pixel rotation method using secret image pixels (11, 10, 01 and 00) is represented in tables 2 and 3.

TABLE II

Lookup table for Pixel Rotation method- pixels 11 and 10























































































	P1				P2			
								
Probability	1/4	1/4	1/4	1/4	1/4	1/4	1/4	1/4
S_1								
$S_1^{270^\circ}$								
S_2								
$S_1 \otimes S_2$								
$S_1^{270^\circ} \otimes S_2$								

TABLE III
Lookup table for Pixel Rotation method- pixels 01 and 00

	P1		P2		P1		P2	
								
Probability	1/4	1/4	1/4	1/4	1/4	1/4	1/4	1/4
s_1								
$s_1^{270^\circ}$								
s_2								
$s_1 \otimes s_2$								
$s_1^{270^\circ} \otimes s_2$								

Encryption and decryption process for this method using two secret image is discussed below with diagram in Fig. 3.

Encryption:

Read two secret image (C_1 & C_2) of size $M \times M$.

Then every pixel comparison of C_1 & C_2 needs here.

As per the lookup table and comparison result, form the blocks s_1 and s_2 .

From s_1 create another block say s_1' by rotating s_1 by 270° .

Finally form the shares S_1 , S_2 and S_1^θ by using s_1 , s_2 and s_1' blocks.

Decryption:

Read the shares S_1 , S_2 and S_1^θ .

Get the secret image C_1 by superimposing S_1 and S_2 shares.

Get the secret image C_2 by superimposing S_1^θ and S_2 shares.

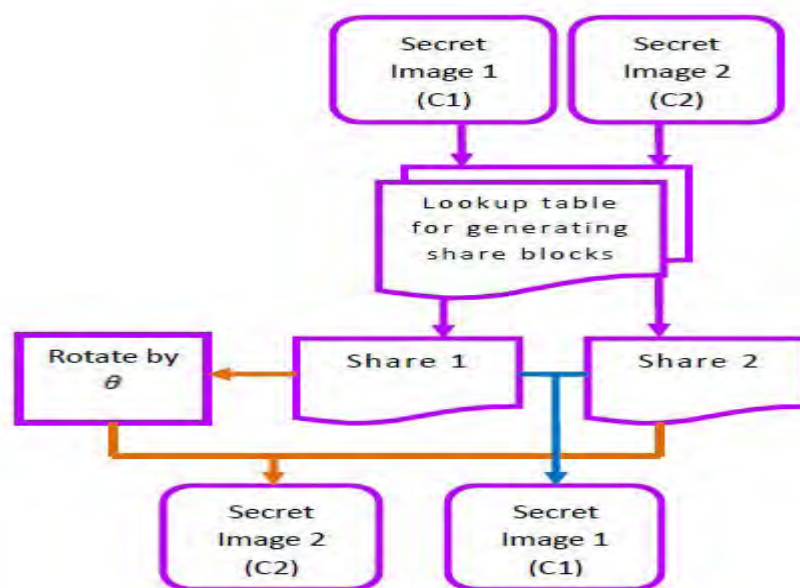


Fig. 3. Encryption and Decryption process of Pixel rotation method

Sample results for this method with three shares are shown in Fig. 4. Here input images are divided into three shares and then combined to get output image.

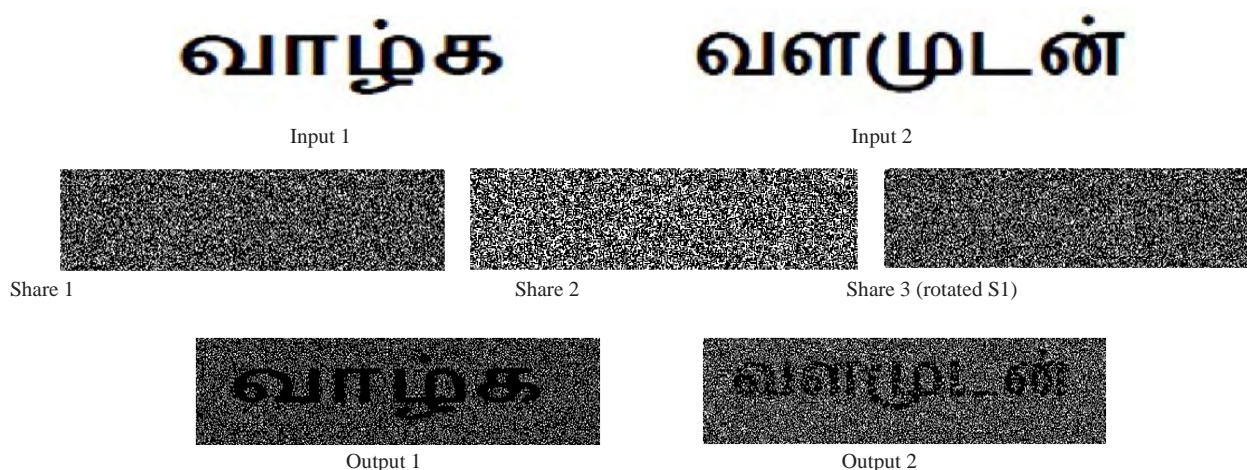


Fig. 4. A sample result for Pixel rotation method

C. Method 3- Share Rotation

Three secret image sharing is explained here. In this method, three secret images are transmitted by sharing it into two shares (S1 & Sref), out of this; one is taken as reference share (Sref). From this reference share create two shares say S2 and S3 offered that the OR operation result of these two gives Sref.

The direction of share rotation plays the major role here. Share1 is rotated in clockwise and counter clockwise direction and these results are stacked with share reference gives the secret image 2 and 3 (C2 & C3). Secret Image1 (C1) is achieved by superimposing S1 with Sref. Table 4 gives the lookup table for generating share blocks in this method using pixels of secret image.

TABLE IV
Lookup table for Share Rotation method using pixels

Pixel of the first secret image	1	1	1	1	0	0	0	0
Pixel of the second secret image	1	1	0	0	1	1	0	0
Pixel of the third secret image	1	0	1	0	1	0	1	0
2x2 block of share 1								
2x2 block of share Ref								
Stacked block by shares 1 and Ref								
share 1'								
Stacked block by shares 1' and Ref								
share 1''								
Stacked block by shares 1'' and Ref								

Encryption and decryption process for this method using three secret image is discussed below with diagram in Fig. 5.

Encryption:

Consider three secret image (C1, C2 and C3) of size $M \times M$.

Compare every pixel of C1, C2 and C3.

Then create the blocks s1 and sref from the look up table.

Make other two blocks s2 & s3 from sref provided that s2 OR s3 creates sref.

Finally create the shares S1, Sref, S2 and S3 and transmit the shares S1, S2 and S3.

Decryption:

Read the shares S1, S2 and S3

To get Sref, perform OR operation in S2 and S3.

Stack S1 and Sref to attain the first secret message C1.

To attain C2, rotate S1 270° clockwise and combine it with Sref.

To attain C3, rotate S1 270° anti- clockwise and combine it with Sref.

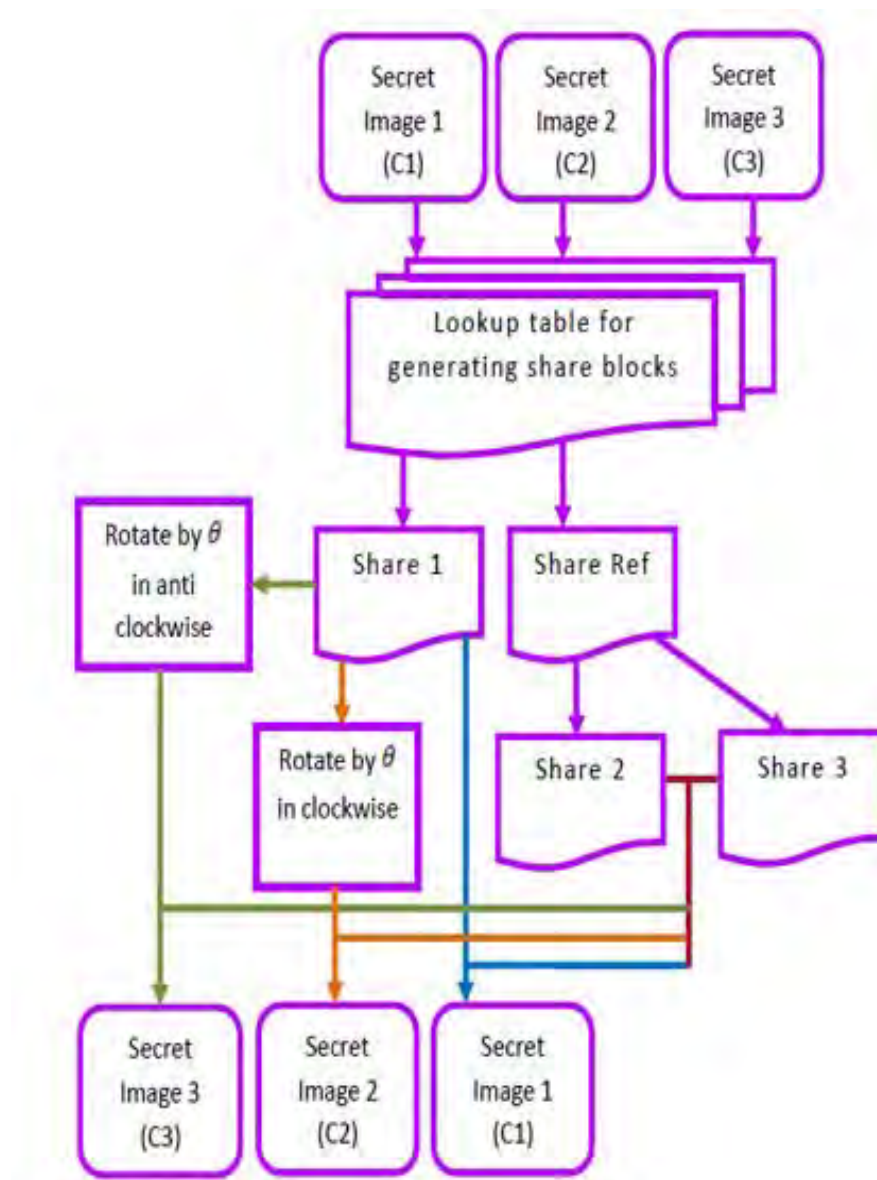


Fig. 5. Encryption and Decryption process of Share rotation method

Sample results for this method with three shares are shown in Fig. 6. Here input images are divided into three shares and then combined to get output image.

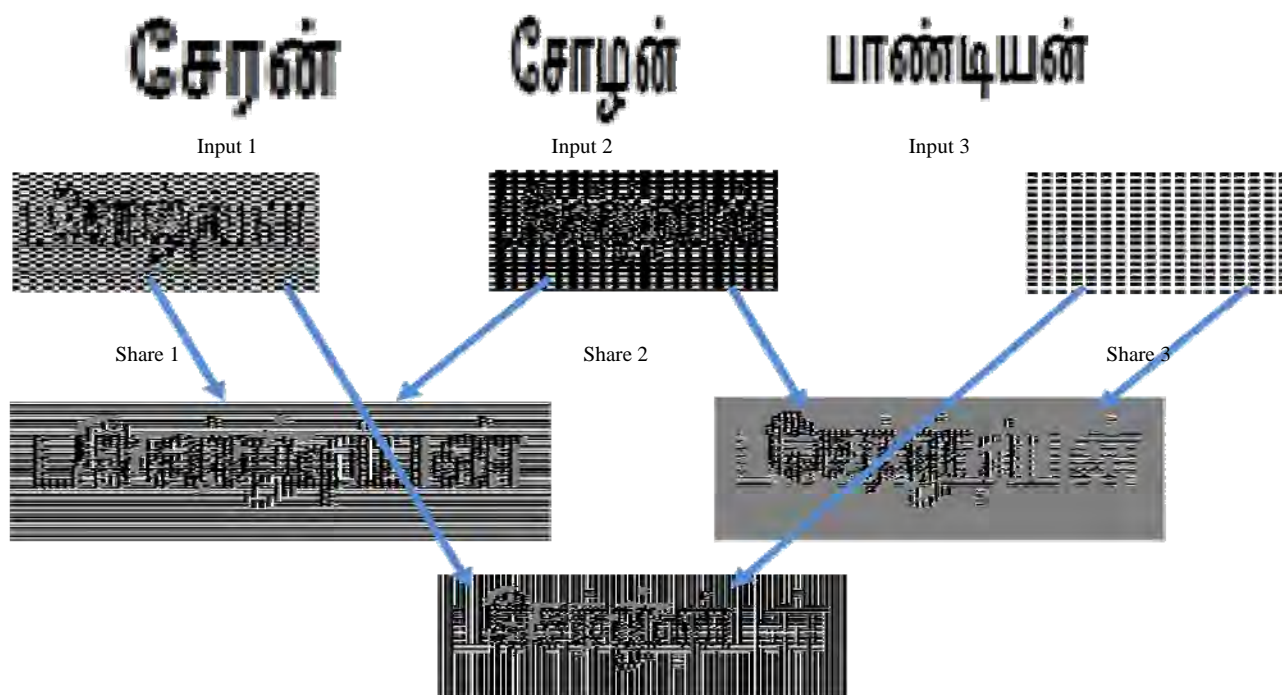


Fig. 6. A sample result for Share rotation method

ADVANTAGES

Without acquainting superfluous troubles it overcomes cheating predicament

Feasibleness

Probability of finding transparencies is greatly minimized

Applicable for distribution system

Each block possesses superior visual quality

III. CONCLUSION

Visual speaks a lot than hearing, each and every one in this world gathering bulk of information with the help of vision. Lot of fields are available to hide confidential information, they are cryptography, steganography, visual cryptography, watermarking and so on. Let us visualize about visual cryptography; Visual Cryptography is an extraordinary encryption technique to camouflage information in images in such a way that it can be decrypted by the human vision if the correct key image is used. In this paper we discussed about three methods of visual cryptography scheme, they are (k,n) scheme, pixel rotation and share rotation. Visual cryptography is an upraising field; some applications of visual cryptography are remote electronic voting, banking customer identification and key management. In future each and every field requires data security, during that time visual cryptography will enhance its applications with the help of its methods.

ACKNOWLEDGMENT

Authors wish to thank J.H.S.Karthikesh, M.Nirup Reddy and Ch.Sri Harsha Kaushik, B.Tech ECE and P. Archana, V. Rajesh, G. Devipriya ACS students of ECE Department, School of Electrical & Electronics Engineering for their TIME, Technical and linguistic support.

REFERENCES

- [1] Schneier, B., 2007. Applied Cryptography: Protocols, Algorithm and Source Code in C. 2nd Edn., Wiley, India.
- [2] Noar, M. and A. Shamir, 1995, Visual cryptography, In: A. De Santis (Ed.), Advance in Cryptography: Eurpocrypt'94, Lecture Notes in Computer Science, 950: 1-12.
- [3] Bert W. Leung, Felix Y. Ng and Duncan S. Wong, 2009. On the security of a visual cryptography scheme for color images. Pattern Recognition, 42: 929-940.
- [4] Chang-Chou Lin and Wen-Hsiang Tsai, 2003. Visual cryptography for gray-level images by dithering techniques. Pattern Recognition Letters, 24: 349-358.
- [5] Chen, T. H., Chin-Chen Chang, Chang-Sian Wu, Der-Chyuan Lou, 2009. On the security of a copyright protection scheme based on visual cryptography. Computer Standards & Interfaces, 31: 1-5.
- [6] Chen, Y. C., Du-Shiau Tsai, Gwoboa Horng, 2012. A new authentication based cheating prevention scheme in Naor-Shamir's visual cryptography. Journal of Visual Communication and Image Representation, 23: 1225-1233.

- [7] Jaafar, A. and A. Samsudin, 2013. An improved version of the visual digital signature scheme. International Arab Journal of Information Technology 10 (6) (In Print)
- [8] Jin, X. and J. Kim., 2012. A secure image watermarking using visual cryptography. Lecture Notes in Electrical Engineering 203 LNEE, pp. 179-187.
- [9] Rastislav Lukac, and Konstantinos N. Plataniotis, 2005. Bit-level based secret sharing for image encryption, Pattern Recognition, 38: 767–772
- [10] Shyong Jian Shyu, Shih-Yu Huang, Yeuan-Kuen Lee, Ran-Zan Wang and Kun Chen, 2007 Sharing multiple secrets in visual cryptography, Pattern Recognition, 40: 3633-3651.
- [11] Wu, C.C and L.H. Chen, 1998. A Study On Visual Cryptography, Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C.,
- [12] Young-Chang Hou, 2003. Visual cryptography for color images. Pattern Recognition, 36: 1619-1629.
- [13] Yuan, Z.-L., G. S. Xia, J. Q. Liu and Z. Han, 2012. Cheat immune and traceable visual cryptography scheme. International Journal of Digital Content Technology and its Applications 6: 226-237.