XOR-BASEDVISUAL CRYPTOGRAPHY

Nidhin Soman[1] and Smruthy Baby[2]

[1] Student,Department of Computer Science And Engineering, MBITS, Nellimattom,
[2]Assistant Professor, Department of Computer Science And Engineering, MBITS, Nellimattom

ABSTRACT

Visual cryptography scheme is a cryptographic technique which allows visual information.It is solve the poor visual quality problem. XOR-based VC. Actually, two XOR-based VC algorithms are proposed, namely XOR-based VC for general access structure (GAS) and adaptive region incrementing XOR-based VC. to be encrypted in such a way that the decryption can be performed by the human visual system,without the help of computers. There are diverse visual cryptography schemes developed based on different factors like pixel expansion, meaningless or meaningful shares, contrast, security, type of secret image and the number of secret images encrypted. This paper discusses most of the visual cryptography schemes and the performance measures used to evaluate them

KEYWORDS

Visual cryptography, random grid, pixel expansion, extended visual cryptography,XOR general access structure, region incrementing, pixel expansion, adaptive security level

1. INTRODUCTION

The world today relies on the internet for information storage, transmission and retrieval. Because of these huge amount of multimedia information is transmitted over the internet. For example, various confidential data such as military maps and commertial identifications are transmitted over the internet. While using secret images security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want. To deal with security problems of secret images, various image secret sharing schemes have been developed.

Visual cryptography is introduced by first in 1994 Noar and Shamir. Visual cryptography is a cryptographic technique which allows visual information to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement.

Visual cryptography is a powerful visual secret sharing scheme in which a secret image is distributed among some participants by dividing the secret image into two or more noise-like shares (or shadow images). When the shares on transparencies are stacked (superimposed) together, the original secret image will be revealed without any mechanical devices like a computer. Decryption can be done using the Human Visual System The process of visual

DOI: 10.5121/ijci.2016.5228

cryptography proposed by Naor and Shamir discusses a technique for encrypting a binary secret image into *n* shares (printed on transparencies), where each pixel is expanded *m* times. Each participant will get a share image but the secret image cannot be revealed with any one share. Any n participants can compute the original secret when any *k* (or more) of them are stacked together. No group of *k-1* (or fewer) participants can compute the original secret.

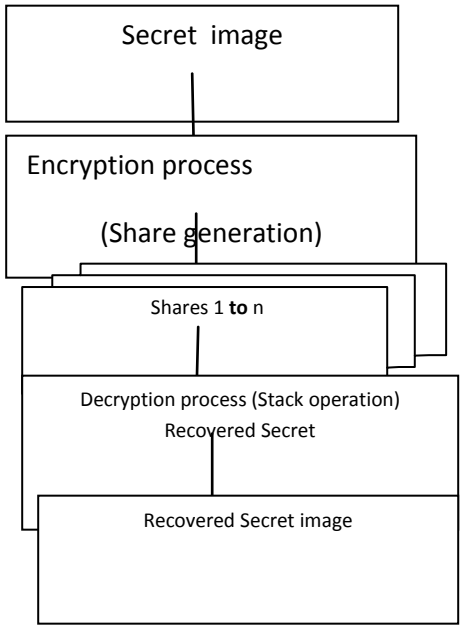

Figure 1: Basic flowchart of Visual Cryptography

The secret image cannot be seen from one transparency, but when *k* or more transparencies are stacked together the image will begin to emerge as the contrast between the black and white pixels becomes sufficient that the human.Initially the secret image is encoded (i.e. shares are generated) and during decoding the k or n shares are stacked together (according to the *(k, n)* or *(n, n)* scheme discussed later) to reveal the secret image. The secret image will get visible to the human visual system. In the *(k, n)* visual cryptography scheme, two collections of *(n* x *m)* Boolean matrices (Basis matrices), C0 and C1 are used. To share a white (black) pixel, the dealer randomly selects one row of the Boolean matrix C0 (C1) and assigns it to the corresponding share image. The gray level and contrast of the m sub-pixels in each of the n share images is defined by the chosen row. The major drawbacks of visual cryptography include pixel Expansion.

2. TRADITIONAL VISUAL CRYPTOGRAPHY

Secret is something which is kept from the knowledge of any but the initiated or privileged. Secret sharing defines a method by which a secret is distributed among a group of Secret pixel Share 1 Share 2 Stacked (OR operation)participants, whereby each participant is allocated a piece of the secret. This piece of the secret is known as a *share*. The secret can only be reconstructed when a sufficient number of shares are combined together. While these shares are separate, no information about the secret can be accessed. That is, the shares are completely useless while they are separated. Within a secret sharing scheme, the secret is divided into a number of shares and

distributed among n persons. When any *k* or more of these persons (where k ≤ n) bring their shares together, the secret can be recovered. However, if *k -1* persons attempt to reconstruct the secret, they will fail.

Due to this threshold scheme, we typically refer to such a secret sharing system as a *(k, n)*-threshold scheme or k-out of- n secret sharing, where n is the number of Total Participant and k is the number of Qualified Participant The basic model for visual sharing of the k out of n secret image. *A (k, n)* VSS scheme is a method by which the shared image (printed text, handwritten notes, pictures, etc.) is visible by k or more participants by stacking their transparencies with the help of an overhead projector. To share a white pixel, the dealer randomly chooses one of the matrices in C0 and to share a black pixel, the dealer randomly chooses one of the matrices in C1. The chosen matrix defines the colour of the *m* sub-pixels in each one of the *n* transparencies. The major drawback is the pixel expansion and low contrast of the reconstructed secret image

3. EXTENDED VISUAL CRYPTOGRAPHY

In visual cryptography, it is also obvious that, while the shares appear to be random (and, in fact, can be shown to contain no informational content that can be used to recover the original secret image on their own), the shares also have no interesting content that could be used to carry other information (such as a biometric image) that might be helpful in a security context. For example, if a share image could be selected to be the finger-print of the share holder, this could be useful in authenticating a user's right to hold that share when the parties meet to combine their share images to reveal the secret. In 1996, Ateniese, Blundo, and Stinson proposed extended visual cryptography (EVC) schemes that can construct meaningful share images. More security is provided for the shares as a cover image is provided for it. For example, if one of the shares of a finger print is covered by another person's finger print then the outsiders may think that the covered share is the original secret image of the finger print

Extended Visual Cryptography (EVC) takes the idea of visual cryptography further by creating shares which are meaningful to anyone who views them. This helps to alleviate suspicion that any encryption has taken place and also presents visually pleasing shares which incorporate all the previously mentioned features of VC. It allows the construction of visual secret sharing schemes within which the shares are meaningful as opposed to having random noise on the shares. After the sets of shares are superimposed, this meaningful information disappears andthe secret is recovered. Meaningful shares avoid attention of hacker considering the security issues over the communication channels. EVCS can also be viewed as a method of steganography. One scenario of the applications of EVCS is to evade the custom inspections, because the shares of EVCS are meaningful images, hence there are fewer chances for the shares to be suspected and detected. In case of EVCS, shares were simply generated by replacing the white and black sub-pixels in a traditional VCS share with transparent pixels and pixels from the cover images, respectively. This scheme provides meaningful share images but endure pixel expansion problem

3.1 RANDOM GRIDS BASED VISUAL CRYPTOGRAPHY

Random grid (RG) is a method to implement visual cryptography (VC) without pixel expansion. RG is defined as a transparency comprising a two-dimensional array of pixels, where each pixel can be fully transparent (white) or totally opaque (black), and the choice between the alternatives is made by a coin-flip procedure. Half of the pixels in a RG are white, and the *remaining pixels* are black. Encoding an image by random grids was introduced initially in 1987 by Kafri and Keren. A binary secret image is encoded into two noise-like transparencies with the same size of

the original secret image, and stacking of the two transparencies reveals the content of the secret. Comparing RGs with basis matrices, one of the major advantages is that the size of generated transparencies is unexpanded. The RG scheme is similar to the probabilistic model of the VC scheme, but the RG scheme is not based on the basis matrices

3.2 COLOUR VISUAL CRYPTOGRAPHY SCHEMES

Up to 1996, visual cryptography schemes were only applied to binary images. Rijmen and Preneel have introduced a visual cryptography scheme for colour images. In their scheme, each pixel of the colour secret image is expanded into a 2×2 block in order to generate two share images. Each 2×2 block on the share image is filled with red, green blue and white respectively, and thus no clue about the secret image can be recognized from any one of these two shares alone. Verheul and Van Tilborg introduced another method for encrypting a coloured image, called *c*-colour (*k*,*n*)-threshold scheme. In this scheme one pixel is expanded into m sub-pixels, and each sub-pixel is partitioned into c colour regions. In each sub-pixel, exactly one colour region will be coloured, and all the remaining colour regions are black. The colour of one pixel is based on the interrelations between colures of the stacked sub-pixels. For this coloured visual cryptography scheme with c colours, the pixel expansion m is c x 3.

Colour Decomposition: In this, every colour on a colour image can be decomposed into three primary colours: C, M,Y (if subtractive model is used) or R, G, B(if additive models used). This method expand every pixel of a colours secret image into a 2 x 2 block in the sharing images and keep two coloured and two transparent pixels in the block

3.3 PROGRESSIVE VISUAL CRYPTOGRAPHY

Progressive Visual Cryptography takes into consideration the premise of perfect secret recovery and high quality secret reconstruction. Many of the schemes do require computational effort in order to perfectly reconstruct the secret. A new sharing concept emerged known as “Progressive Visual Cryptography” which revealed the secret image progressively as more and more number of shares were stacked together.

3.4 REGION INCREMENTING VISUAL CRYPTOGRAPHY

In traditional visual cryptography scheme, one whole image is considered as a single secret and same encoding rule is applied for all pixels of one image. So it reveals either entire image or nothing. It may be the situation that different regions in one image can have different secrecy levels, so we can't apply same encoding rule to all pixels. Ran-Zan Wang developed a scheme Region Incrementing Visual cryptography for sharing visual secrets of multiple secrecy level in a single image . In this scheme, different regions are made of a single image, based on secrecy level and different encoding rules are applied to these regions

3.5 SEGMENT BASED VISUAL CRYPTOGRAPHY SCHEME

Traditional visual cryptography schemes were based on pixels in the input image. The limitation of pixel based visual cryptography scheme is loss in contrast of the reconstructed image, which is directly proportional to pixel expansion. Bernd Borchert proposed a new scheme which is not

pixel-based but segment-based. It is useful to encrypt *messages* consisting of symbols represented by a segment display. For example, the decimal digits 0, 1, 9 can be represented by seven-segment display. The advantage of the segment based encryption is that, it may be easier to adjust the secret images and the symbols are potentially easier to realize for the human eye and it may be easier for a no expert human user of an encryption system to understand the working. The secret, usually in the form of digits is coded into seven segment display before encrypted. Two random share images will be generated during encryption. Decryption process involves the stacking of these two share images

3.6 DYNAMIC VISUAL CRYPTOGRAPHY

The core idea behind dynamic visual cryptography is increasing the overall capacity of a visual cryptography scheme. This means that using a set of two or more shares,we can potentially hide two or more secrets. Multiple secret sharing is very useful when it comes to hiding more than one piece of information within a set of shares.

4. XOR VISUAL CRYPTOGRAPHY

A (k, n) visual cryptographic scheme encrypts a secret image into n share images (printed on transparencies)distributed among n participants. When any k participants stack their shares on an overhead projector (OR operation),the secret image can be visually discovered by a human visual system without the aid of computers (computation).But the monotone property of OR operation reduces the visual quality of reconstructed secret image for OR-based VCS. Generally all the conventional visual cryptography schemes (VCS) uses OR operation for stacking operations and so it is also called OR-based VCS. But it offers a poor visual quality image during decoding (stacking). Major advantage of XOR-based VCS (XVCS), is that since it uses XOR operation for decoding which results into exact recovery of the secret

4.1PROBABILISTIC VISUAL CRYPTOGRAPHY SCHEMES

In this scheme, usually there is no pixel expansion, i.e., m is The reconstruction of the image however is probabilistic, meaning that a secret pixel will be properly reconstructed only with a certain probability. On the other hand, in the deterministic model the reconstruction of an approximation

5. GENERAL ACCESS STRUCTURES (GAS)

In *(k, n)* scheme, using any of the 'k' shares someone can decode the secret image which in turn reduces security . To overcome this issue the basic model is extended to general access Structures by G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson [, where an access structure is a specification of all qualified and forbidden subsets of 'n' shares. Any subset of 'k' or more qualified shares can decrypt the secret image but no information can be obtained by stacking lesser number of qualified shares or by stacking disqualified share[1].

5.1THE PROPOSED ALGORITHM FOR GAS

Comparing to conventional VC, advanced properties such as good resolution, contrast and colour are provided by XOR-based VC at the expense of utilizing light-weight computational devices. Nowadays, light weight devices such as cell phones and smart devices are popular. XOR-based VC is possible to be widely used in the future. Some state-of-the-art works on XOR-based VC ,, are confined to threshold cases. Designing VC method for GAS becomes more necessary. An access structure, denote as *(TQual,TForb)*, is required in the proposed algorithm. When an access structure is given ,the basis *T*0 can be obtained. We construct the XOR-based VC for GAS based on the basis *T0*. Diagram of the proposed XOR-based VC for GAS is depicted in FIG2:The share generation is a pixel-wise operation, and *n* shared pixels are constructed via the proposed algorithm for every given secret pixel. Simply, the proposed algorithm consists of two components: the generation of *t* pixels and the construction of remaining $n - t$ pixels

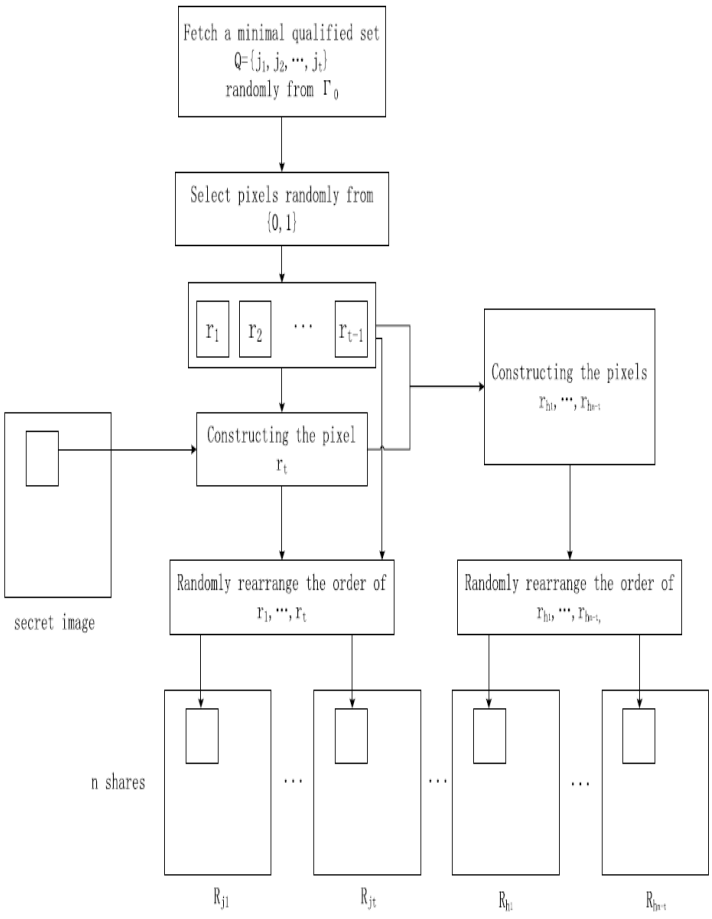

Figure 2.Diagram of the xor based vc Gas

Input: a binary secret image S with $M \times N$ pixels, and an access structure $(\Gamma_{Qual}, \Gamma_{Forb})$.
Output: n shares $R_1, \ldots, R_n$.
Step 1: Obtaining the basis Γ_0 of the access structure $(\Gamma_{Qual}, \Gamma_{Forb})$. Denote L as the number of minimal qualified sets in the basis Γ_0.
Step 2: For each position (i, j) in the secret image, n shared pixels $R_1(i, j), \ldots, R_n(i, j)$ are generated by Steps 3-7.

Step 3: Randomly select a minimal qualified set $Q = \{j_1, \ldots, j_t\}$ in the basis Γ_0.
Step 4: Construct $t - 1$ pixels $r_1, \ldots, r_{t-1}$ by

$$\begin{cases} r_1 = Random(\bullet) \\ \cdots \\ r_{t-1} = Random(\bullet) \end{cases} \tag{3}$$

where procedure *Random* return a value randomly chosen from {0, 1}.
Step 5: Construct the tth pixel by

$$r_t = S(i, j) \oplus r_1 \oplus \cdots \oplus r_{t-1} \tag{4}$$

where symbol $\oplus$ denotes the Boolean XOR operation.
Step 6: Rearrange the order of $r_1, \ldots, r_t$ and assign the values of the rearranged pixels to $R_{j_1}(i, j), \ldots, R_{j_t}(i, j)$.
Step 7: The remaining $n - t$ pixels are constructed by

$$\begin{cases} r_{h_1} = S(i, j) \oplus r_1 \oplus \cdots \oplus r_{t-1} \oplus r_t \\ r_{h_2} = S(i, j) \oplus r_1 \oplus \cdots \oplus r_{t-1} \oplus r_t \oplus r_{h_1} \\ \cdots \\ r_{h_{n-t}} = S(i, j) \oplus r_1 \oplus \cdots \oplus r_{t-1} \oplus r_t \oplus r_{h_1} \oplus \cdots \oplus r_{h_{n-t-1}} \end{cases} \tag{5}$$

where $h_1, \ldots, h_{n-t}$ are the $n - t$ indices in $\{1, \ldots, n\} - \{j_1, \ldots, j_t\}$. Pixels $r_{h_1}, \ldots, r_{h_{n-t}}$ are assigned to the shared pixels $R_{h_1}(i, j), \ldots, R_{h_{n-t}}(i, j)$, respectively.
Step 8: Output the n shares $R_1, \ldots, R_n$.

Figure 3. XOR-based VC for General Access Structure.

5.2 ADAPTIVE REGION INCREMENTING XOR-BASED VC

In the proposed method, the concept of *adaptive security level* is introduced. In the previous methods the security levels in the secret image are revealed in accordance with the quantity of stacked shares. Every share is with the same priority. For the *adaptive security level*, the security levels are reconstructed according to the qualified set in which the members can be specified by the sharing strategy. Different shares are with different priorities. XORbased VC with adaptive security *level* property is named as adaptive region incrementing XOR-based VC.

To construct the adaptive region incrementing XOR-based VC, algorithm proposed in the former section is adopted. For each minimal qualified set Q, Q is assigned an initial security level. Based on the initial security levels of the minimal qualified sets, security levels of the remaining qualified sets are calculated by Security Level Assignment algorithm . When the assignment finishes, shares of the adaptive region incrementing XOR-based VC are constructed. Usually, the XOR-ed result by shares in a qualified set reveals the associated security levels while the XOR-ed result by shares in a forbidden set cannot.

Herein, we describe the generation of shares for the adaptive region incrementing XOR-based VC. Diagram of this method is depicted in Fig. 4. A binary secret image with k security levels $L1$, . . . , Lk are considered as input, as well as minimal qualified sets in t_0 assigned with initial security levels. First of all, the remaining qualified sets, which are not assigned the initial security levels, are automatically given the associated security levels by the assignment algorithm. When the security level assignment completes, the share construction begins. The construction is an approach derived from the XOR-based VC for GAS. Similarly, it comprises two parts: the construction of t pixels and the generation of the remaining $n - t$ pixels.

For each time, a pixel s is constructed based on the security level of given secret pixel. A qualified set, which contains t participants, is randomly chosen from the set of qualified sets.
At the next step, $t - 1$ shared pixels are constructed randomly, and the tth shared pixel is generated based on the $t - 1$ random pixels and pixel s. The remaining $n - t$ shared pixels are iteratively constructed by pixel s and the former shared pixels that have been assigned values. Similarly, the iterative generation of the $n - t$ shared pixels helps enhancing the visual quality. Herein, the security level assignment algorithm is given as follows.

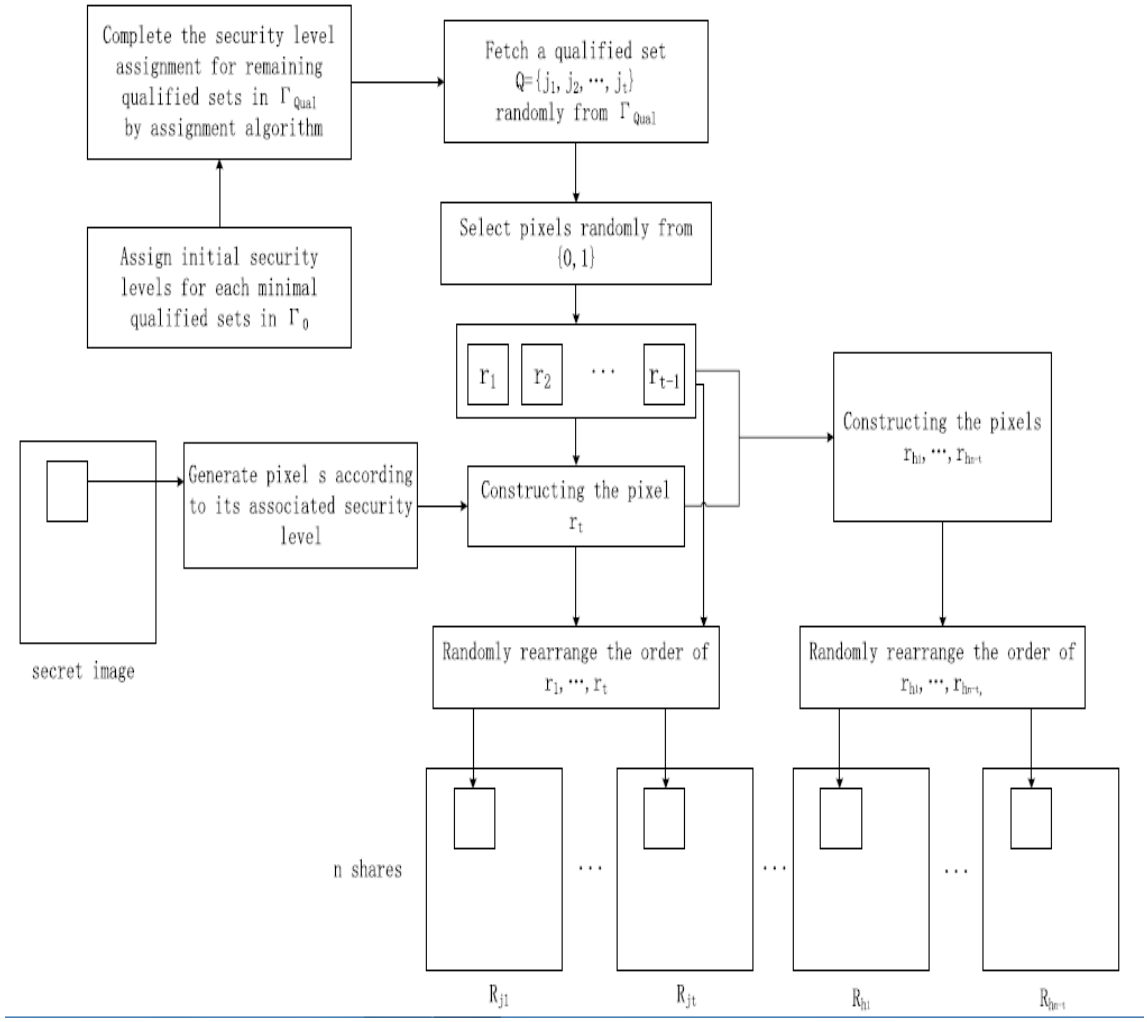

Figure. 4. Diagram of the adaptive region incrementing XOR-based VC.

Input: An access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ whose minimal qualified sets are with initial security levels.
Output: Qualified sets in Γ_{Qual} with assigned security levels.
Step 1: For each qualified set $Q \in \Gamma_{Qual}$ which is not assigned the security level, obtain qualified sets $A_1, \ldots, A_m \subset Q$.
Step 2: If all the qualified set $A_1, \ldots, A_m$ are with assigned security levels, get the highest security level L_t $(1 \leq t \leq k)$ from $A_1, \ldots, A_m$. If not, the assignment for Q is processed later until each qualified set in $A_1, \ldots, A_m$ is assigned a security level.
Step 3: Determine the security level L of Q by

$$L = \begin{cases} L_{t+1}, & \text{if } t < k, \\ L_t, & \text{otherwise.} \end{cases}$$

Step 4: Generate a pixel s according to L_d by

$$s = \begin{cases} 0, & \text{if } S(i, j) \in L_0 \text{ or } y > d, \\ 1, & \text{otherwise.} \end{cases} \quad (8)$$

Step 5: Construct $t - 1$ pixels $r_1, \ldots, r_{t-1}$ by

$$\begin{cases} r_1 = Random(\bullet) \\ \cdots \\ r_{t-1} = Random(\bullet) \end{cases} \quad (9)$$

where procedure *Random* return a value randomly chosen from {0, 1}.
Step 6: Construct the tth pixel by

$$r_t = s \oplus r_1 \oplus \cdots \oplus r_{t-1} \quad (10)$$

where symbol $\oplus$ denotes the Boolean XOR operation.
Step 7: Rearrange the order of $r_1, \ldots, r_t$ and assign the values of the rearranged pixels to $R_{j_1}(i, j), \ldots, R_{j_t}(i, j)$.
Step 8: The remaining $n - t$ pixels are constructed by

$$\begin{cases} r_{h_1} = s \oplus r_1 \oplus \cdots \oplus r_{t-1} \oplus r_t \\ r_{h_2} = s \oplus r_1 \oplus \cdots \oplus r_{t-1} \oplus r_t \oplus r_{h_1} \\ \cdots \\ r_{h_{n-t}} = s \oplus r_1 \oplus \cdots \oplus r_{t-1} \oplus r_t \oplus r_{h_1} \oplus \cdots \oplus r_{h_{n-t-1}} \end{cases} \quad (11)$$

where $h_1, \ldots, h_{n-t}$ are the $n - t$ indices in $\{1, \ldots, n\} - \{j_1, \ldots, j_t\}$. Pixels $r_{h_1}, \ldots, r_{h_{n-t}}$ are assigned to the shared pixels $R_{h_1}(i, j), \ldots, R_{h_{n-t}}(i, j)$, respectively.
Step 8: Output the n shares $R_1, \ldots, R_n$.

Figure 5.Security Level Assignment

6. RELATED WORK

In this paper XOR based cryptography is applied to both text and video.some of the Data hiding algorithms can be applied to secure the image This paper has applications in military, bank etc the construction of the pixel is based on the random value..This is a new technique.For example,

we consider one department head and two department researchers for sharing a secret with two security levels. The department head has the prime priority that he can reveal the whole secret by using his share and one of the two shares held by the researchers. But the two researchers only can recover the first security level in the secret by their two shares. information hiding algorithm can be used for the Security. There could be a chance to get man in middle attack, then shares can be protected using a key. This key can be automatically generated. This key can be protected by another encryption and decryption .In this shares some of the texts are embedded and are hidden and its implementation is very easy.

7. PERFORMANCE ANALYSIS

There are various parameters used to evaluate the performance of visual cryptography scheme.
Pixel expansion- Pixel expansion m refers to the number of sub-pixels in the generated shares that represents a pixel of the original secret image. It represents the loss in resolution from the original secret image to the shared one.
Contrast- Contrast is the relative difference in weight between combined shares that come from a white pixel and a black pixel in the original image. Contrast of the recovered secret image must be adjusted so that it is visible to the human eye.

Security- Security is satisfied when each share individually discloses no information of the original image and the original image cannot be reconstructed with shares fewer than k in(k, n) scheme.

Accuracy- Accuracy is measured to be the quality of the reconstructed secret image and evaluated by peak signal-to-noise ratio (PSNR). Mean Squared Error (MSE) can also be used for accuracy evaluation

8. CONCLUSIONS

Visual cryptography offers perfect security for all the digitally transmitted secret images. This paper discusses various visual cryptography schemes and commonly used performance evaluation parameters. Diverse visual cryptography schemes were developed based on different factors like pixel expansion, meaningless or meaningful shares, contrast, security, type of secret image (either binary or colour) and the number of secret images encrypted. In this paper, we further exploit the extended capabilities for XOR-based VC. In essence, two XOR-based VC algorithms, namely XOR-based VC for GAS and adaptive region incrementing XOR-based VC, are introduced. For the first method, complicated sharing strategy by using GAS can be implemented

REFERENCES

[1] Xiaotian Wu and WeiSun (2015)Extended Capabilities for XOR-Based Visual Cryptography.
[2] G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson, “Visualcryptography for general access tructures”, Proc.ICAL96,Springer, Berlin, 1996, pp.416-428.
[3] T. Chen and K. Tsao, “User-friendly random-grid-based visual secret sharing”, IEEE Trans. Circuits Syst. Video Technol., vol.21, no. 11, pp. 1693_1703, Nov. 2011
[4 P. Tuyls, H. Hollmann, J. Lint, and L. Tolhuizen, “XOR-based visual cryptography schemes”, Designs, Codes, Cryptography,vol. 37, no. 1, pp. 169_186, 2005.

[5] C. Blundo, A. De Santis, and M. Naor, "Visual cryptography for grey level images," Inf. Process. Lett., vol. 78, no. 6, pp. 255–259, Nov. 2000
[6] C. Blundo and A. De Santis, "Visual cryptography schemes with perfect reconstruction of black pixels," Comput. Graph., vol. 22, no. 4,pp. 449–455, Aug. 1998.
[7] C.-N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognit. Lett., vol. 25, no. 4, pp. 486–494, Mar. 2004.
[8] X. Wu and W. Sun, "Random grid-based visual secret sharing for general access structures with cheat-preventing ability," J. Syst. Softw., vol. 85,no. 5, pp. 1119–1134, May 2011
[9] S. J. Shyu, "Visual cryptograms of random grids for general access structures," IEEE Trans. Circuits Syst. Video Technol., vol. 23, no. 3,pp. 414–424, Mar. 2013
[10] C.-N. Yang, H.-W. Shih, C.-C. Wu, and L. Harn, "k out of n region incrementing scheme in visual cryptography," IEEE Trans.Circuits Syst. V
[11] C.-N. Yang and D.-S. Wang, "Property analysis of XOR-based visual cryptography," IEEE Trans. Circuits Syst. Video Technol., vol. 24, no. 2,pp. 189–197, Feb. 2014
[12] M. Naor and A. Shamir, "Visual cryptography," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 950. Berlin, Germany:Springer-Verlag, 1995, pp. 1–12.
[13] F. Liu and C. Wu, "Embedded extended visual cryptography schemes,"IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 307–322,Jun. 2011
[14] 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
[15] R.-Z. Wang, "Region incrementing visual cryptography," IEEE Signal Process. Lett., vol. 16, no. 8, pp. 659–662, Aug. 2009

AUTHOR

NIdhin Soman. is currently pursuing M.Tech in Computer Science and Engineering in Mar Baselios Institute of Technology And Science Nellimattom. He completed his B.Tech from,. Mar Baselios Institute of Technology And Science, Nellimattom. His areas of research are Network Security and Image Processing.

Smruthy Babyreceived B.TechDegree from Mahatma Gandhi University in 2008 and M.Techin computer science and engineering from Anna.University. Currently working as Assistant professor at Mar Baselios Institute of Technology And Science,.Her research interest include Network Security and Image Processing.