# Literature Review Of Shamir's Secret Sharing for Image Encryption

**Vikash Rawat (BT17CSE019)**

**Harish Dutt(BT17CSE026)**

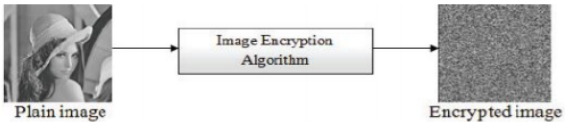
## Abstract:

With the increasing use of the network technology and internet applications, the protection of digitized data has become a priority so that unauthorized access can be stoped. In order to over come this problem,A lot of secret image sharing schemes have been introduced. Secret image sharing scheme is a method used for the protection of the digitalized image against illegal access. The secret image is divided into many secret shares in such a way that each share does not reveal any sensitive information to unauthorized user. In this paper, we studies some methods of secret image sharing which explains the new approaches and challenges. This paper also provides a comparative analysis of different methods based on different properties.

## Introduction:

Multimedia can be a form of text, photograph, audio, video and much more. Industries, whether hospitality, aviation, banking, insurance, science and technology ,military etc. uses multimedia for communication , it is being used in every field, either for publishing something or for some other purpose. It can be seen that the dependency of every person toward internet for sharing information made the privacy over internet as a prime goal which need to be solved to protect and safely transfer data over the network. Digital image is a form of multimedia which is shared over the internet by lots of user and it is necessary to provide security, privacy and integrity to the user. So image encryption plays important role to protect from any unauthorized user access.

The image encryption techniques and the data encryption techniques are not same. And there are lots of security related problems with processing and transmissions of digital image, so it is necessary to maintain the quality and the security of the image. Also images are less sensitive compare to data because change in single pixel does not have much effect on original image. In other words a small change in image is acceptable compared to data but it is more vulnerable to the attackers.




**Some of the secret image sharing methods are as follow:**

**Method 1: XOR Based Secret Image**

**Sharing Scheme with Security Improvement ∗ 1Javvaji V.K. Ratnam, 2T. Sreenivasulu Reddy, 3P. Ramana Reddy**

Algorithm 1: **Share Image Generation**:

Input: Original image = I

Output: n shares ={ $S_1, S_2, S_3, \ldots, S_n$ , }

Step 1: random image R = random(255)

Step 2: XOR of random image with secret image C = R I where, denotes bit-wise Boolean XOR operation.

Step 3: Dividing C by k G = C / k, where, k is the minimum number of shares for reconstruction of secret and k n.

Step 4: Generation of n random numbers ri = random (255), for i = 1 to n

Step 5: Generation of n identifiers xi= [4-bitLSB(ri) 4bit(MSB(ri)], for i = 1 to n

Step 6: Generation of n share images Si = circularrightshift(G, xi), for i = 1 to n

Algorithm 2: **Secret image reconstruction**

Input: n shares ={ $S_1, S_2, S_3, \ldots, S_n$ , }

Output: Reconstructed secret image,I1

Step 1: Combining k share images Y = 0

Y = Y + circularleftshift(Si, xi) , from i = 1 to n

Step 2: Reconstruction of secret image

I1 = Y C

**Method 2: Chen ET algorithm**

Algorithm 1 **Sharing Procedure.**

Input : { $I_1, I_2 \cdots I_n$} . are n secret images

Output : { $S_1, S_2, S_3, \ldots, S_n, S_{n+1}$ } are n + 1 shared images

1. Random matrix generation T

T=Random (0, 255)

2. Computing n − 1 random matrices { B1, B2 · · · Bn− 1} using XOR operation

Loop (i=1 to i<=n-1){

Bi = Ii $\bigoplus$ T,

}

3. Generating shared images

S1 = T

S2 = B1

Loop (i=3 to i<=n){

Si = Bi $\bigoplus$ Bi− 1

}

Sn+1 = I1 $\bigoplus$ Bn− 1

Algorithm 2: **Recovery Procedure**.

Input: { $S_1, S_2, S_3, \ldots, S_n, S_{n+1}$ } are n + 1 shared images

Output: { $R_1, R_2 \ldots R_N$ } , n recovered images

1. Compute first recovered image using XOR operation R1=S1 $\bigoplus$ S2 $\bigoplus$ S3 $\bigoplus \cdots \bigoplus$ Sn

2. find n − 1 random matrices { B1, B2 · · · Bn− 1} using XOR operation

B1 = S1

Loop(k=2 to k<=n-1){

Bk = Sk $\bigoplus$ Bk− 1

}

3. Recovery of remaining secret images

{ R2, R3 · · · Rn}

Loop(k=2 to k<=n){

Rk = Bk $\bigoplus$ S1 ,

}

**Method 3: The Thien–Lin (*r*, *n*) SIS scheme**

Algorithm 1: **Encoding secret image**

Input: Secret image O(m pixels)

Output: Encode O to n shadows images { $S_1, S_2, S_3, \ldots, S_n$ , }

Step 1: Truncate pixels of image

If pixel values in O>250

Set pixel values=250

O'=image after truncation

Step 2: Q=permutation (all pixels in O'), Q is the result image after permutation

Step 3: set current processing section number j to 1

Step 4: r non-processed pixels a0,a1,a2,. . . ,ar-1 of Q are taken sequentially to form a section j

Create polynomial , degree(r-1) :

$f_j(x)=(a_0+a_1x+a_2x_2+\ldots+a_{r-1}x_{r-1})\bmod 251.$

Step 5:generate n pixels:

$f_j(1), f_j(2), f_j(3), \ldots, f_j(n)$,

assign them to n shadow images $S_1, S_2, S_3, \ldots, S_n$ .

Step 6: j=j+1

Step 7: goto step 4 and repeat from there until all pixels of Q are processed

Algorithm 2:**Recovery procedure**

Input: r shares,shadow images { $S_1, S_2, S_3, \ldots, S_r$ }

Output: original image

Step 1: current processing section : set section number j to 1

Step 2: from each r shadow images take one non processed pixel

Step 3: using these r pixels find $f_j(1), f_j(2), f_j(3), \ldots, f_j(r)$,

and use Lagrange interpolation to find the coefficient $a_0, a_1, a_2, \ldots, a_{r-1}$

in equation, $f_j(x)=(a_0+a_1x+a_2x_2+\ldots+a_{r-1}x_{r-1})\bmod 251$.

$a_0, a_1, a_2, \ldots, a_{r-1}$ these coefficient correspond to r pixel values of htr jth section in Q

step 4: j=j+1

step 5: goto step 2 and repeat from there until all pixels of shadow images are processed $\{ S_1, S_2, S_3, \ldots, S_r \}$

step 6:inverse-permutation operation to Q = secret image(O')

**Method 4: A New (k, n) Secret Image Sharing Scheme (SISS) Amitava Nag1 , Sushanta Biswas2 , Debasree Sarkar2 , and Partha Sarkar2**

Algorithm 1: **The initialization phase**

Step 1: D=dealer

D chooses p and q (two large prime numbers)

$N= p \times q$

Step 2: D select integer g, $g \in [(N)^{1/2}, N]$

And g is relative prime to p and q

And { g, N} is public key

Step 3: P= $\{ P_1, P_2 \ldots P_N \}$ , participants

Loop (i=1 to i<=n) {

$k_i$ = randomly select an integer from the interval [2, N]

}

Each $P_i$ correspond $k_i$ representing its own secret shadow

Compute: $Z_i = ((g)^{ki})\bmod N$

Then each $P_i$ Supply $Z_i$ and identity number $Id_i$ to D via public channel

Step 4: for $P_i$ and $P_j$ , if $i \neq j$ then $Z_i \neq Z_j$ , D must ensure that

If $Z_i \neq Z_j$ : then ank $P_i$ toselect another $k_i$ from the interval [2,N]

Step 5: { $id_i$,$Z_i$} are made public

Algorithm 2: **Shares construction mechanism**

Input: (a)Secret Image $(H \times W)_{size}$

(b) k ($k \geq 3$) and n

Output: n shadows images $\{ S_1, S_2, S_3, \ldots, S_n, \}$ of size (H× W)

Step 1: D chooses an integer $k_0$ randomly

$Gcd(k_0,p)=1$

Gcd($k_0$,q)=1

Find d such that d× $K_0$=1mod$\phi$ (N)
,

$\phi$ (N) is the Euler phi-function.

Step 2:D compute following:

(a) $Z_0$ =(g $^{k0}$) modN and $I_i$ =($Z_i$ $^{k0}$) mod N for each

Participant $P_i$ make ($Z_0$,d) public

(b)selects a hash function H and generates $M_i$ for each $P_i$

Step 3: Divide secret image into T non –overlapping blocks { $B_r$} from r=1 to T;

Each $B_r$ is of 1× k pixels, where $T = (H \times W)/k$

Step 4: i= 1

Step 5: r=1

Step 6: find sum of k consecutive pixels { $R_1$,$R_2$,$R_3$... $R_k$} of block $B_i$ with the help of i$^{th}$ Prüfer sequence as

$$S_i = \sum_{j=1}^{k} C_j \; R_j$$

Where $\forall_j = 1 \ldots k, C_j = m + 1$

m=frequency of j in i$^{th}$ Prüfer sequence

step 7: (a) $b^p_{M-1}, \ldots b^p_1 b^p_0$ are bit sequence of size $M = (k-2)\log_2 k$ from $i^{th}$ Prüfer sequence

$b^i_j$ {0, 1 .

(b) $b^S_B, \ldots b^S_1 b^S_0$ are bit sequence of size B = (4k-M) from $S_i$

(c)In step 2(b), $M_i$ is generated,Divide it into k-non overlapping blocks $D_r$ of size B bits , where

1≤ r≤ k, k× B× | $M_i$ | | .| represent cardinality

and $D_r = b^H_{B-1}, \ldots b^H_1 b^H_0$

(d) perform X-OR operation between $S_i$ and $D_r$ b bit sequence $b'_{B-1}, \ldots b'_1 b'_0$ ,where r=1 to k

Each is repeated for X-OR operation with $S_i$ after ever k blocks of original secret image

(e) Obtain a number $N_c$ of 4k bits long by appending the bit sequence $b'_{B-1}, \ldots b'_1 b'_0$ at the end of the sequence $b^p_{M-1}, \ldots b^p_1 b^p_0$ as $N_c = b^p_{M-1}, \ldots b^p_1 b^p_0 = b'_{B-1}, \ldots b'_1 b'_0$

Step 8:Obtain $N_1$ *and* $N_2$ two 4k bit numbers

$$N_1 = b^1_{4k-1}, \ldots b^1_1 b^1_0$$

$$N_2 = b^2_{4k-1}, \ldots b^2_1 b^2_0$$

Such that

$$b_{4k-1} b_{4k-2 \ldots .} b_1 b_0 = b^1_{4k-1}, \ldots b^1_1 b^1_0 \text{ Å } b^2_{4k-1}, \ldots b^2_1 b^2_0$$

Step 9: concatenate $N_1$ *and* $N_2$ and obtain 8k bit sequence as

$$b^i_{8k-1}, \ldots b^i_1 b^i_0 = b^1_{4k-1}, \ldots b^1_1 b^1_0 \text{ Å } b^2_{4k-1}, \ldots b^2_1 b^2_0$$

Step 10:

$p_1^i = b_7^i, \ldots b_1^i b_0^i$

$p_2^i = b_{15}^i, \ldots b_9^i b_8^i$

. . . . . .

. . . . . .

$p_k^i = b_{8k-1}^i, \ldots b_{8k-7}^i b_{8k-8}^i$

And these values are assign to $i^{th}$ shadow

Step 11: r=r+1

Step 12: goto step 6 and repeat the process until r>T for the $i^{th}$ Prüfer sequence

Step 13: i=i+1

Step 14: goto step 5 and repeat the process until i>n.

The dealer D each time performs the above steps to generate a new secret image $I_s$ and generates n encrypted share images { $S_1, S_2, S_3, \ldots, S_n$ , }

Algorithm 3: **Recovery phase with verification**

Input: Any k share images { $S_1, S_2, S_3 \ldots S_n$ } of size H× W and the value of k

Output: Original Secret Image $I_s$ ,size H× W

Step 1: For each $P_i$ find

$I_i' = Z_0^{k_i} \bmod N$ to get the share

Step 2: Each $P_i$ in P can be verified

$I_i'$ provided by $P_i$ and test $I_i'^d = Z_i \bmod N$

If the test is successful, then $P_i$ is legal participant and share Si is accepted and then goto step 3

Else exit

Step 3: Each Pi generates $M_i' = H(I_i')$ . $M_i'$ is divided into k non-overlapping blocks $D_r$ ($1 \leq r \leq k$ ) of size B=(4k-M) bits, where M =(k - 2) $\log_2$ k and , k× B× | $M_i$ |

Step 4: Divide each shadow image $S_i$ into T number of non-overlapping blocks $\{B_r^i\}_{r=1}^{T}$ of 1× k pixels, where $T = (H \times W)/k$ and 1 ≤ i ≤ k

Step 5: r=1

Step 6: i=1

Step 7: For k consecutive pixels $P_1^i P_2^i \ldots\ldots P_k^i$

$p_1^i = b_7^i, \ldots b_1^i b_0^i$

$p_2^i = b_{15}^i, \ldots b_9^i b_8^i$

. . . . . .

. . . . . .

$p_k^i = b_{8k-1}^i, \ldots b_{8k-7}^i b_{8k-8}^i$

Step 8: concatenate the bits stream of all k pixels and find a bit sequence of size 8k as $b_{8k-1}^i, \ldots b_1^i b_0^i$

Step 9: Divide the 8k bits sequence into two, 4k bit sequence as $N_1$ and $N_2$

$N_1 = b^1_{4k-1}, \ldots b^1_1 b^1_0$

$N_2 = b^2_{4k-1}, \ldots b^2_1 b^2_0$

Step 10: Obtain one 4k bits sequence $N_c = b_{4k-1} b_{4k-2} \ldots b_1 b_0$ as $b_{4k-1} b_{4k-2} \ldots b_1 b_0 = b^1_{4k-1}, \ldots b^1_1 b^1_0$ Å $b^2_{4k-1}, \ldots$

Step 11: Extract first (from MSB) M bits stream from $N_c$ and generate a Prüfer sequence { $f_1 f_2 \ldots f_{k-2}$ } . The remaining (4k - M) bits of $N_c$ and (4k - M) bits of $D_r$ ( $D_r$ is generated in step 3) are XORed and generates a number $S_i$

Step 12: find linear equation

$$\sum_{j=1}^{k} C_{ij} \; R_j \; = S_i$$

Where $\forall_j \; = 1 \ldots k, C_j = m + 1$

m=frequency of j in $i^{th}$ Prüfer sequence

step 13: i=i+1

step 14: goto step 7 and repeat the process until i>k

step 15: k number of linear equations are created as created in step 12

step 16:use these k equations to get $R_1 R \ldots R_k$

these value correspond to k pixel values of the secret images $I_s$

step 17:goto step 6 and repeat the process until r>T

| Parameters | V.K. Ratnam, T. Sreenivasulu Reddy, P. Ramana Reddy | Chen and wu | Thien–Lin | Amitava Nag1 , Sushanta Biswas2 , Debasree Sarkar2 , and Partha Sarkar2 |
|---|---|---|---|---|
| Secret Images | n | n | n | n |
| Shared Images | n | n+1 | n | n |
| Recovery Type | Lossless | Lossless | Lossy | Lossless |
| Sharing Type | Rectangle | Rectangle | Rectangle | Rectangle |
| Security | High | Average | Average | High |
| Color Depth | Gray | Gray | Gray | Gray and color |

**Fig: Comparison between four methods of secret image sharing**

## Conclusion

Image plays an important role in everybody lives and they are used in many ways in our daily lives. Therefore it is necessary to maintain the integrity and confidentiality of the digital image that being transmitted over the network. Some of the image encryption techniques using secret sharing has been discussed that plays an important role in image transmission. In this paper a review of some important secret image sharing techniques provided in last decades. This techniques are studied and analyzed well. In its own way ever technique is unique and is suitable for many applications. Everyday new techniques are evolving which are fast and secure and these encryption techniques work with high security rate. This review provide comparative analysis of different secret image sharing technique based on different properties.

## References


- Chen, Tzung-Her, and Chang-Sian Wu. ” Efficient multisecret image sharing based on Boolean operations.”
- Lin, Tsung-Lieh, et al. ” A novel visual secret sharing scheme for multiple secrets without pixel expansion.” Expert systems with applications
- XOR Based Secret Image Sharing Scheme with Security Improvement ∗ 1Javvaji V.K. Ratnam, 2T. Sreenivasulu Reddy, 3P. Ramana Reddy
- A New (k, n) Secret Image Sharing Scheme (SISS) Amitava Nag1 , Sushanta Biswas2 , Debasree Sarkar2 , and Partha Sarkar2
- Thien CC, Lin JC: Secret image sharing. *Compt. Graph*
- Multi Secret Image Sharing Scheme based on DNA
    - Cryptography with XOR
- Arthanari S., Mastan M., and Bagank B., “Chaotic Image Encryption using Modular Addition and Combinatorial Techniques,” The International Arab Journal of Information Technology,
- Chen C. and Fu W., “A Geometry-based Secret Image Sharing Approach,” Journal of Information Science and Engineering,
- Jing Qiu and Ping Wang, “ Image encryption and authentication scheme” , IEEE, Computational Intelligence and Security
- K-n secret sharing visual cryptography scheme for color image using random number by Shyamalendu kandar ;Arnab maiti:
- An Efficient K-N Secret Sharing Image and AES Encryption Algorithm in Visual Cryptography by Vignesh. M, Raihana. P.A, Shahadha Hakkim, Sukanya:
- Encryption On Grayscale Image For Digital Image Confidentiality Using Shamir Secret Sharing Scheme