Randomly Tampered Image Detection and Self-Recovery for a Text Document Using Shamir Secret Sharing

Sudha M S, Thanuja.T C

***Abstract* -Forgery of the digital image is to hide or to remove some meaningful or useful information of the image. In this paper (k,n) Shamir threshold scheme is applied to an image where the tampering is done randomly all over the image. Performance parameters are checked with the random tampering. Comparative study of algorithm for different block sizes ispresented. The algorithm is checked for four different block sizes 2x2, 2x4, 3x3, 2x5. Effect of these blocks sizes on stego image and reconstructed image is observed.PSNR is calculated for various block sized algorithm andthe visual quality is compared.**

Keywords- Randomtampering, Threshold, Shamir secret sharing

I. INTRODUCTION

Digital image authentication plays a significant role for security services in computer and communication application. In this digital world wherein many a transaction are carried out online, authentication of the document is of paramount importance because digital images can be easily tampered to manipulate the important content, which will lead to disastrous consequence.As for checking the integrity and authenticity of digital images many a scheme, have been proposed and improved upon regularly.

In the process of communication, if a part of the information in digital image documentis falsified, detection of doctored area in the image and subsequently restoring the original information has become highly indispensable task. To protect documents like scanned checks, gold bond certificates, signed documentsetc, tamper detection and repairing technique is essential.

In any document images alphabets, lines, boxes are the major components. These components are digitized into two major gray values one is background values and foreground values. Back ground values are dominantly blank spaces and foreground values are text, linesetc. such images look like binary. After processing, the binary like gray scale document imagedestroys the smoothness in the boundaries of textcharacters, resulting in visually poorperception. This makes authentication difficult for `1binary natured images. To circumvent the above challenge, an efficientalgorithm for semi fragile watermarking is proposed. In this paper (k, n) threshold secret sharing scheme is applied to randomly tampered image. This scheme is used to detect the tampered area as well Simulation results are discussed.

Sudha M S, Research Scholar, Jain University, Bengaluru, India

Thanuja.T C, Professor, VTU, Belgaum, India

II. LITERATURE REVIEW

Concept of secret sharing is first presented by Shamir [1]. He made use of polynomial method to generate the shares. All these shares are put together to recover the secret message.Lin, C.C., Tsai, W.H [2] proposed (k, n) secret sharing threshold method where k is the minimum number of shares required to recover the secret out of n shares. Pei-yulin and chi-shiangchan [3] used (k, n) secret sharing threshold method to detect the cheater during secret retrieval process .He has proposed a verifiable secret image sharing scheme that can resist dishonest participants. Che-Wei Lee et.al [4] has proposed a blind authentication method based on Shamir secret sharing. Authentication of the digital document is achieved using this scheme. An algorithm is developed for tamper detection and localization using Shamir secret sharing. Using inverse Shamir scheme a self-repair of tampered data is achieved. Li Bai saroj Biswas et.al[5] used an another scheme along with Shamir secret scheme called matrix projection secret sharing scheme to divide image into n shares out of n ,k shares are sufficient to recover the secret image. This scheme is effective, reliableand secure method to prevent the secret image frombeing lost, stolen or corrupted.Mohammad JavadKhosravi [6] presented a novel stenography technique based on secret sharing and wavelet transform to develop an algorithm which is stable against many attacks and high authentication capability against counterfeiting. In recent years Pei Luo and Andy Yu-Lun Lin [7] has proposed AMD architecture (algebraic manipulation detection)to protect Shamir secret sharing scheme module from attackers and cheaters.AMD scheme is implemented on FPGA to improve the security level under fault injection attack.Angelina Espejelet.al [8] proposes a secret sharing technique to prevent flaws in security.Bichat Chiewthanakul et.al [9] uses Shamir secret sharing schemes to facilitatedistributed trust or shared control for critical activities by gating thecritical action on cooperation by k of nusers.ShuiHuaet.al [10] has focused on watermarking for RFID system. A fragile watermarking technique is developed for RFID tag.Algorithm has developed for tamper detection of RFID tag and locates modification in RFID system.

III. (K,N) THRESHOLD SECRET SHARING

Proposed method explainsthe generation of stego image, authentication and secret recovery, self-repair of tampered image.

A. Generation of stego image.

Steps to develop stego image is as follows:

1) The Input image which is in any format i.e. GIF, TIFF, and JPGetc. are converted into PNG format

978-1-5090-0774-5/16/$31.00 © 2016 IEEE

(32 bit) with alpha channel. This alpha channel has default value of 255(8 bits) during creation so that it provides complete transparency for the image. The input image is binarised using threshold scheme.

2) The binarised image is divided into number of small blocks. Each block is of mxn size,m may be equal or not to n. Number of partial shares obtained are p, where p=mxn. Authentication signals are generated using (k,n)threshold secret-sharing scheme giving rise to p number of shares.
3) These P shares are randomly distributed in the alpha channel. The random distribution of share is done along with the secret-key. The resulted image is stego-image.Fig.1explains the generation of stego image.

Algorithm1: To generate stego image

1) To generate a stego image, secret d is in the form of integer is taken and number of participants or shares are n and threshold k≤ n. Prime number *p* is chosen such that *p* is larger than *d.*
2) Select (k-1) integer values say C_1, C_2, C_3, C_4..... Ck-1within the range of 0 through (p-1).
3) Select n distinct real values x_1 ,x_2 , x_3.....x_n.(k-1) degree polynomial to compute n values of $F(x_i)$,
4) Following $(k-1)$ equation is to compute n function values $F(x_i)$, called partial shares for i=1,2,3.4……n

i.e. $F(x_i) = (d + c_i x_i + c_i {x_i}^2 + \cdots \ldots + c_{k-1} {x_i}^{k-1}) mod\ p$…….(1)

These coefficients are solved in order to recover the secret. Which is explained in section B

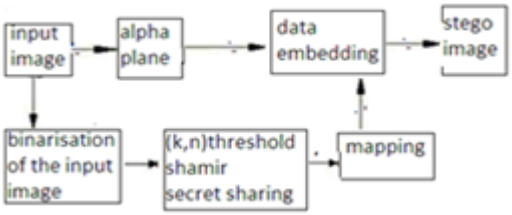


Fig.1: Generation of stego image

B. *Authenticationand secret recovery*

The authentication procedure will be followed to make sure none of the pixels are varied from the source image. If varied, those pixels are marked in black which forms the output of authentication procedure.Fig.2 explains the complete flow graph of authentication and secret recovery. The process of each block is explained below.

1) Transmittedstego image is binaries. And authentication signals are generated using secret sharing scheme.
2) The generated authenticated signals are compared with values in alpha channel which is present in the first column of same block. If the signals match with each other, the block is said to be non-tampered and hence authenticated. If not matched, the whole block is marked with black colour indicating tamper. Tampered blocks are sent for repair. This process is continued till the end of the image is reached**.**

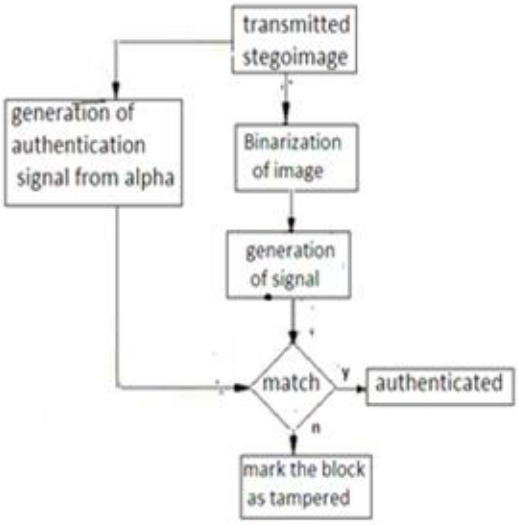


Fig.2: Authentication and secret recovery

1) Algorithm 2: Secret recovery.

At output K shares are collected from the n participants. *Shares* are used to set up $(x_1, F(x_1)), (x_1, F(x_1)), \ldots\ldots (x_k, F(x_k))$

$F(x_j) = (d + c_1 x_j + c_2 x_j^2 \ldots\ldots c_{k-1} x_j^{k-1})$ mod p.

Where j = 1, 2,3.....*k.*

Solve the k equation from the above using Lagrange's interpolation to obtain *d* as follows

$$.d = (-1)^{k-1}[F(x_1)\frac{x_2 x_3 \ldots\ldots x_{k-1}}{(x_1-x_2)\,(x_1-x_3)\ldots\ldots(x_1-x_k)}$$

$$+F(x_2)\frac{x_1 x_3 \ldots\ldots x_{k-1}}{(x_2-x_1)\,(x_3-x_1)\ldots\ldots\ldots(x_1-x_k)}$$

$$\ldots F(x_k)\frac{x_1 x_2 \ldots\ldots x_{k-1}}{(x_k-x_1)\,(x_k-x_2)\ldots\ldots\ldots(x_k-x_{k-1})}]mod\ p$$

C) Repairing procedure

Oncethe authentication process is completed.The repairing process needs to be undertaken. Repairing process is a methodology adopted to reconstruct the base image using the signals embedded in the image. Fig.3flow diagram shows localising and repair procedure.

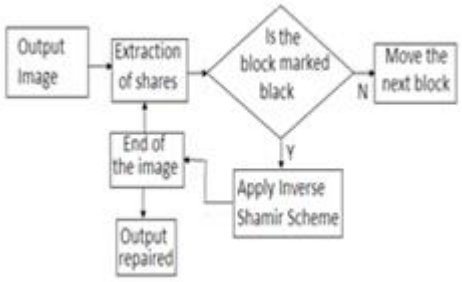


Fig.3:Repair procedure

The each block of flow diagram is explained below.

Once the tampered images are marked, the next process is to repair the tampered image to retrieve the original image.

1. All the partial shares are extracted from the alpha channel using the secret key that was used to embed **the partial signals.**

2. Out of the n partialshares extracted, two of the shares are selected which do not originate from a tampered block preferably.
3. Inverse Shamir algorithm to calculate share $A_{0=}(-1)^{k-1}\left[f(x_1)\frac{x_2x_3\ldots.x_k}{(x_1-x_2)(x_1-x_3)\ldots..(x_1-x_k)}+ f(x_2)\frac{x_1x_3\ldots.x_k}{(x_2-x_1)(x_2-x_3)\ldots..(x_2-x_k)}\ldots+ f(x_k)\frac{x_2x_3\ldots.x_{k-1}}{(x_k-x_1)(x_k-x_2)\ldots..(x_k-x_{k-1})}\right]modp$

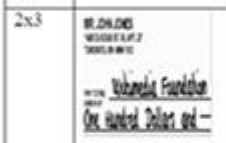
After obtaining the decimal authentication signals, they are converted to binary to form 8-bit string. These eight bits represent the binary value of pixels P1 to Pn in mxn pixel block.

IV. EXPERIMENTAL RESULTS

Experimental results for best reconstructed image haslisted as follows. Image of any size is considered as input or original image as shown in Figure.4 and the generated stego image is shown in Figure.5. Randomly tampered image is shown in Figure.6 and detected tampered image is shown in Figure.7. Reconstructed image is shown in Figure.8

V. COMPARISION OF DIFFERENT BLOCK SIZES AND DATA REPAIR CAPABILITY, PSNR

TABLE I:
COMPARATIVE STUDY OF DIFFERENT BLOCK SIZE SAND PSNR

Block division	Watermarked image(tampering ratio30%)	PSNR of watermarked image	Reconstructed image
2x2		36.2328	
2x3		32.118	
2x4		31.21089	

Visual quality of stego image and effective repair capability of the tampered image depends on the block size of the binarisied image .Larger the block size like 2x3,2x4,2x5will reduce the visual quality of the stego image. Therefore PSNR reduces, because of more number of shares embedded in the alpha channel reduces transparency in the cover image. On the other hand it increases the data repair capability with smaller block size like 2x2. In smaller the block size lesser the number shares embedded in the alpha channel, hence transparencyincreases, correspondingly PSNR .In contrary less number of shares are inadequate to repair the tampered data. Therefore repair capability decreases.This is proved in Table.I

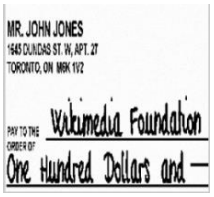


Fig.4:original image Fig.5:stego image

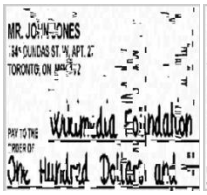


Fig.6:Tampered image Fig.7:Tamper detectedimage

Fig.8:Reconstucted image

VI. ROBUSTNESS VERIFICATION

To check robustness of the algorithm for random tampering, two attacks are applied.

A. Superimposing attack

TABLE II: PARAMETERS OF SUPERIMPOSING ATTACK
(IMAGE SIZE: 256X256)

No of blocks	No of tampered Blocks.(Tampered ratio	No of recovered blocks (detection ratio)	(RR) No of Repaired block	FAR	FRR
4096	615(15%)	615(100%)	604 98.21%	0%	0%
4096	1024(25%)	1024(100%)	763 (74.60%)	0%	0%
4096	1884(45.12%.)	1884(100%.)	814 (55.85%)	0%	0%

Superimposing attack operation is done by imposing different data on certain area in the image in such away it destroys the alpha channel.From Table2 it is noted that detection ratio are 100% due to ease in detection of the alpha channel value 255 at image part attacked by superimposing. Higher tampering ratio reduces the repair capability. Following table shows tabulation of parameters.

B. Painting attack.

The content of a stego image may be painted in some areas. It is noted here that, when a stego-image is tampered

by painting, which does notchange the content of the alpha channel plane, the hidden authentication signals and data for repairing are not destroyed.

TABLE III
PARAMETERSOF PAINTING ATTACK (IMAGE SIZE:256X256)

No of blocks	No of tampered Blocks.(Tampered ratio)	No of recovered blocks (detection ratio)	(RR) No of Repaired block	FAR	FRR
4096	205(5%)	1850(90.20 %)	100%	9.7 %	0 %
4096	410(10%)	340(82.90 %)	100%	17.02%	0 %
4096	820(20.019%)	600(75.8%)	100%	24.21%	0 %

Therefore, the computed authentication signals from the alpha channel values are always true, and as long as the computed authentication signal is not identical to the extracted authentication signal for a block, the block will be marked as having been tampered with. this explains why the false rejection rate is 0%.

VII. CONCLUSION

Experimental results have been shown to prove the effectiveness of the proposed method. Robustness is verified using paint attack and superimposing attack. The proposed algorithm is checked for different block sizes 2x4 2x5,3x3,4x4. From the experimental results we notice that larger the block size improves the data repair capabilty and reduces the precision of stego image.

REFERENCES

[1].A. Shamir, “How to share a secret”, Communications of the ACM, Vol. 22, 1979, pp. 612–613

[2]Lin, C.C., Tsai, W.H.: Secret image sharing with steganography and authentication. J. Syst. Softw 73(3), 405–414 (2004)

[3]Pei-yulinand chi-shiangchan “A Verifiable and Recoverable Secret Image Sharing Mechanism” Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications.

[4]Che-Wei Lee ,Wen-Hsiang Tsai “A Secret-Sharing-Based Method for Authentication of Grayscale Document Images via the Use of the PNG Image With a Data Repair Capability” ieee transactions on image processing, vol. 21, no. 1, January 2012.

[5] Li BaiSarojBiswas, Albert Ortiz Don Dalessandro “An Image Secret Sharing Method” Information Fusion, 9th International IEEE Conference on10-13 July 2006 Florence pp. 1-6.

[6]Mohammad JavadKhosravi, Ahmad Reza Naghsh-Nilchi “ A novel joint secret image sharing and robust steganography method using wavelet ”Published online: 8 October 2013 Springer-Verlag Berlin Heidelberg 2013

[7] Pei Luo and Andy Yu-Lun Lin, Zhen Wang, Mark Karpovsky “Hardware implementation of secure Shamir’s secretsharing scheme” 2014 IEEE 15th International Symposium on High-Assurance Systems Engineering

[8] Angelina Espejel-Trujillo1 , Mariko Nakano-Miyatake1 , Jesus Olivares-Mercado, Hector Perez-Meana1 “a cheating-prevention mechanism for hierarchical secret-image-sharing using robust watermarking” Multimedia Tools Application DOI 10.1007/s11042-015-2701-7 Spinger published on 10 June2015.

[9]BhichateChiewthanakulNattayaneeDarath, SupawadeeWanapongtipakorn “A (t, w)Threshold Scheme over Insecure Channels” the 8th electrical engineering/ electronics, computer, telecommunications and information technology (ecti) association of Thailand - conference 2011.

[10]ShuiHua, Han and Chao-Hsien Chu Tamper Detection in RFID-Enabled Supply Chains Using Fragile Watermarking ShuiHua, Han and Chao-Hsien Chu 2008 IEEE International Conference on RFID The Venetian, Las Vegas, Nevada, USA April 16-17, 2008