Shamir Secret Sharing Based Authentication Method With Data Repair Capability For Gray Scale Document Images Via The Use Of PNG Image

Nagababu Manne[#1], *K.J.Silva Lorraine* [*2]

[#] *Dept. of ECE, Sir C.R.Reddy College of Engineering, AP, India*
[*] *Assistant Professor*
Dept. of ECE, Sir C.R.Reddy College of Engineering, AP, India

Abstract*— Generally digital images are mostly used to preserve confidential & important information. But the problem is providing authentication and integrity to these digital images is a very challenging task. Therefore using this paper a new efficient authentication method is proposed to provide for grayscale document images using the Portable Network Graphics (PNG) image with data repair capability. In this concept an authentication signal generated by each block of a grayscale document image and then using Shamir secret sharing scheme grayscale document image authentication signal and binarized block content is combined and transformed into several shares. These several binarized block content shares are then combined into an alpha channel plane then the PNG image is built from combining the grayscale image with alpha channel plan. In this process the authentication for image is achieved as follows; if the authentication signal measured from the current block content does not match that extracted from the shares embedded in the alpha channel plane then that image block is tampered. Then using reverse Shamir scheme, two shares from unmarked blocks are collected and then data repairing is applied. Finally simulation results are provided to prove the concept of proposed method.

Keywords*— *Data hiding, data repair, grayscale document image, image authentication, Portable Network Graphics (PNG) image, secret sharing

I. INTRODUCTION

Generally digital images are mostly used to preserve confidential & important information. But the biggest problem is providing authentication of digital images especially digital images of documents and it must also requires the capability of repairing the tampered documents. Thus many fields which deals with important agreements, architectural or medical designs, ,law suites, testaments, marks cards, legal documents, cheques, certificates etc requires highly efficient and robust authentication and image repair capability to their digital documents. Generally whenever the documents are scanned, then the images of those documents will have two major gray values as back-ground and the other is fore-ground. These kinds of images are known as binary-like though they are gray scaled. These types of images are gray valued in nature and look like a binary. The advantage with this type of images is it is possible to reduce the size of the image by using the concept of binarization. But the process of binarization creates reduced zig-zag patterns of contours. For the binary images the recognition of tampers is very complex in nature and it is a very challenging task. And while in the process of authentication, combining the authentication signals and binary images causes a lot distortion and the binary nature of binary gray scale images lead to discernible changes after authentication process.

Therefore this paper concentrates on providing an algorithm with a new method for authentication of gray scale document images with the capability of self-repairing for fixing tampered g gray scale image data and parallelly answers the problems in the process of image tampering detection by keeping the visual quality of image. Remaining of this paper prepares as, section I clearly discusses about the digital images of documents and the need for authentication of those documents. In section II we briefly explain the related work already done by several people and the different kinds of authentication schemes. From the section III our required work will be explained clearly i.e. in section III we discusses the algorithms for creating secret shares, recovering of secret shares and algorithm for stego image generation. Image authentication and data repairing is discussed in section IV, which is core part of this paper. Finally section V and VI presents the algorithms for authentication and repairing capability of images. Section VII provides that the effectiveness of the proposed method with simulation results.

II. RELATED WORK

Weighted multi-secret sharing

In 1979 Shamir proposed the concept of secret resource sharing. The Secret sharing schemes are categorized as several classes as per numbers of secrets to be shared. Two well-known basic categories are *single secret and multiple secrets*. Similarly, based on the capability of shares, the concept of secret resource sharing classified as, *same-weight shares and weighted shares.* In *weighted shares* concept while recovering the image different shares have different capabilities, therefore more weighted shares requires less other shares and a fewer weighted shares need higher other shares to recover the secret. Therefore Based on these concept two typical categories can be classified: Polynomial based schemes and Chinese Remainder Theorem (CRT) based schemes. Therefore based on the simple relation presents between the weights of shares and their lengths a new CRT based (w,N) threshold secret sharing scheme is proposed and the partial shares are created using the following equation

$$F(x_i) = \left(d + c_1 x_i + c_2 x_i^2 + \cdots\cdots + c_{k-1} x_i^{k-1}\right) \bmod P \qquad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Here, i=1, 2, 3…n

Using the following equation the secret message will be recovered as.

$$d = (-1)^{k-1}\left[F(X_1)\frac{(x_2 x_3 x_4 \cdots\cdots x_k)}{((x_1 - x_2)(x_1 - x_3)\cdots(x_1 - x_k))}\right] + \left[F(X_2)\frac{(x_1 x_3 x_4 \cdots\cdots x_k)}{((x_2 - x_1)(x_2 - x_3)\cdots(x_2 - x_k))}\right] + \ldots\ldots + \left[F(X_k)\frac{(x_1 x_2 x_3 \cdots\cdots x_k)}{((x_k - x_1)(x_k - x_2)\cdots(x_k - x_{k-1}))}\right] \qquad \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

***Comparisons between CRT based scheme and MIGNOTTE'S scheme*:**

These both schemes are purely based on CRT and these both schemes use same type of process to recover the secret. The weighted multi-secret sharing scheme generates pi × n bit primes for the shares of different weights of pi. Whereas in Mignotte's scheme, first the Mignotte sequence is generated with the length of '*n*' bits and then by multiplying with the pi primes pi×n primes are generated. Then after the generating primes both the schemes use same type of process to gat shares. The differences present in Creating the primes (or co-primes) will affects only the features of performance but not the security features. Advantage of weighted multi-secret sharing scheme is its implementation is straightforward and simple.

Pattern-Based data hiding method binary image authentication

The concept of *"Pattern-Based data hiding method binary image authentication*" is proposed by Huijuan Yang and Alex C. Kot in April 2007. In this new technique the un- even embed ability if digital image by using the embedding of watermark is discussed well. And also the complexity of locating the "embeddable" pixels is discussed and authentication scheme to incorporate authenticity of image is proposed well. The important features of Pattern-Based data hiding method binary image authentication are:

- Good visual quality of the watermarked image is achieved by assessing the flip ability of an image pixel.
- Un-even embed ability of the image is handled carefully by efficiently arranging the watermark only in "embeddable" blocks only.
- Blind watermark extraction is achieved by carefully studying the invariant features in flipping pixels of binary images
- Larger capacity is achieved by partitioning the image in different ways.
- Higher security for the watermarked image is achieved by investigating the location of embeddable pixels

***Two Layer* Binary Image Authentication Scheme**

A *double layer or two layer* binary image authentication schemes is proposed by Alex C and Huijuan Yang. In this concept the first layer is responsible for overall authentication and the second layer for finding the tampering locations of image. In this process the image is sub-divided several multiple macro-blocks that are classified into eight categories. In order to identify the tamper locations of the image block identifier is created for every class of block and integrated in those "qualified" and "self-detecting" macro-blocks. And the entire authentication is achieved in the primary layer (first) by hiding the cryptographic signature (CS) of the image and in the second layer, by integrating the block identifier (BI) in the "qualified" or "self-detecting" macro-blocks the localization of the tampering is achieved. The greatest advantage of *two layer* binary image authentication scheme is effectiveness of the scheme in detecting any changes, and identifying the tampered locations in the image.

III. PROPOSED SYSTEM

Algorithm for Creating Secret Shares

Algorithm 1: (t, n)-threshold secret sharing

Input: In this process consider secret *'c'* as an integer, and '*n'* number of participants such as threshold t ≤ n.

Output: the output is '*n'* shares in the form of an integer for the n participants.

Step1: in this step consider a random prime number *'p',* which is larger than *'c'.*

Step2: choose t-1 integer values m_1, m_2… m_{t-1} between 0 to p-1

Step3: choose n distinct real values $y_{1,2,\ldots\ldots} y_n$

Step 4: by using the following (t-1) degree polynomial equation we can compute n function values f (y_j), known as partial shares, for j=1, 2…..n

$$f(y_i) = \left(c + m_1 y_i^1 + m_2 y_i^2 + \cdots\cdots + m_{t-1} y_{t-1}^{t-1}\right) \bmod p \qquad \ldots\ldots\ldots\ldots\ldots (3)$$

Step5: Then transfer the two tuple $(y_j, f(y_j))$ as a share to the j^{th} participant where j=1, 2, 3……n.

Therefore there are t number of coefficients denoted by c and $m_1$through m_{t-1}. Finally to form t equation to recover secret c, collect t shares from the n participants. The process of solving secret recovery is as

Algorithm 2: Secret recovery of shares

Input: From the n number of participants select t shares and the prime number p whereas p and t both are prime

Output: In the shares, the secret c hidden and coefficients m_j used in $f(y_j)$ where j=1, 2, 3, m- 1.

Step1: in this step the t shares are used as $(y_1, f(y_1)), (y_2, f(y_{2,})), \cdots (y_t, f(y_{t,}))$ to set up

$$f(y_i) = \left(c + m_1 y_i^1 + m_2 y_i^2 + \cdots\cdots + m_{t-1} y_{t-1}^{t-1}\right) \bmod p$$

………………….. (4)

Step2: By using Lagrange's interpolation equation solve the above equations.

$$c = (-1)^{k-1}\left[F(y_1)\frac{(y_2 y_3 y_4 \cdots\cdots y_k)}{((y_1-y_2)(y_1-y_3)\cdots(y_1-y_k))}\right] + \left[F(y_2)\frac{(y_1 y_3 y_4 \cdots\cdots y_k)}{((y_2-y_1)(y_2-y_3)\cdots(y_2-y_k))}\right] + \cdots$$

$$\ldots + \left[F(y_k)\frac{(y_1 y_2 y_3 \cdots\cdots y_k)}{((y_k-y_1)(y_k-y_2)\cdots(y_k-y_{k-1}))}\right] \bmod p$$

………………….. (5)

Step3: Then following equality and comparing the result with (3) in step 1, find out the m_1 through m_{t-1}, while regarding variable y in the equality below to be yj in

$$f(y) = \left[f(y_1)\frac{(y-y_2)(y-y_3)\ldots(y-y_t)}{((y_1-y_2)(y_1-y_3)\ldots(y_1-y_t))}\right] + \left[f(y_2)\frac{(y-y_1)(y-y_3)\ldots(y-y_t)}{((y_2-y_1)(y_2-y_3)\ldots(y_2-y_t))}\right] + \ldots$$

$$+ \left[f(y\ )\frac{(y-y_1)(y-y_3)\ldots(y-y_{t-1})}{((y_t-y_1)(y_t-y_3)\ldots(y_t-y_{t-1}))}\right] \bmod p$$

………………….. (6)

I. IMAGE AUTHENTICATION AND DATA REPAIRING

In the process of authentication and data repairing of image, by using binary grayscale document image E with an alpha channel plane a PNG image is created. Then the original image E is transformed into the binary form specifying the threshold value E_b [10]. To generate n secret shares by using Shamir's secret sharing scheme E_b is used as input. Then the successfully mapped secret shares are combined with alpha channel plane to produce a PNG image with imperceptibility effect. Here the mapped secret shares are randomly combined with alpha channel to provide high security to the image. Then the PNG image created and encrypted using chaotic logistic map [4]. Figure 1 shows the illustration of this process

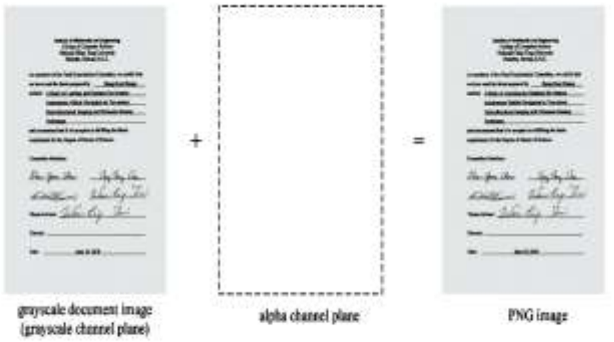


Fig 1. Illustration of creation of a PNG image from a grayscale document image and an additional alpha channel plane

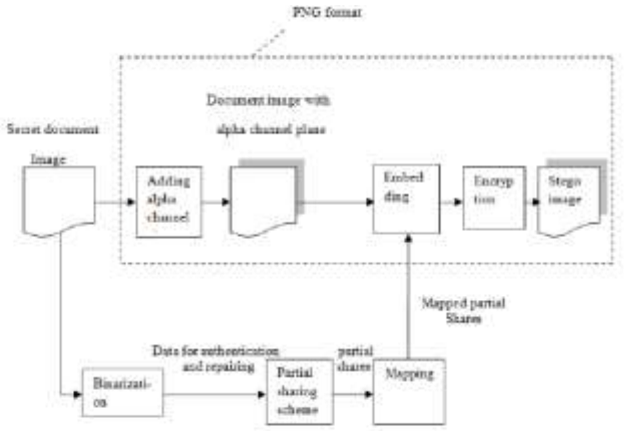


Fig 2: Creating a PNG image from grayscale document image and alpha channel.

Figure 2 shows the process of creating a PNG image from grayscale document image and alpha channel.

Algorithm for Stego-Image Generation

The generation of stego- image as illustrated using the following algorithm.

Algorithm: from a given *grayscale image generating a PNG format* stego image.

Input: an image document E in grayscale with two major gray values and with a secret key K.

Output: encrypted PNG image E' including authentication signal and data repairing capability

Part 1: Authentication signal generation

Step1 Binarization of input image: To get the two representative gray values g_1 and g_2, the Moment preserving threshold [3] is applied to E. The required obtain the threshold value is obtained by averaging the g_1 and g_2. Using this threshold binary version of Eb will calculate by using binarization of E.

Step2 Conversion of cover image into PNG format: By using alpha channel plane E_α the image E is converted into PNG image.

Step3 Starting of loop: Take in a un- refined raster scan order of 2×3 block B_b in E_b with pixels $p_1, p_2, p_3, \cdots p_6$

Step 4 Authentication signal generation: here generate a 2-bit authentication signal $L = b_1 b_2$ with $b_1 = p_1 \oplus p_2 \oplus p_3$ and $b_2 = p_4 \oplus p_5 \oplus p_6$

Part 2: Design and embedding of shares

Step5 Creation of data for secret sharing: In this step the data is created for secret sharing. Here the total 8 bits of $b_1 b_2$ and $p_1, p_2, p_3, \cdots p_6$ forms an 8-bit string and this string is divided into two 4-bit segments, and finally convert the each segment into 2 decimal numbers α_1 *and* α_2 respectively.

Step 6 Generation of partial shares: set $p.m_j, y_j$ following value apply eqn. (1) p=17 (the smallest Prime number larger than 15); 2) $c = \alpha_1$ and $m_1 = \alpha_2$; and 3) y_1=1,y_2=2,……y_6=6. Using equation 1 and threshold secret sharing scheme and generate six partial shares r_1 through r_6 using the following equations:

$$r_j = f(y_j) = (c + m_1 y_j) \bmod p \qquad \text{……… (7)}$$

Step7 Mapping of partial shares: In this step edit 238 to each of $r_1, r_2, r_3, \cdots r_6$ resulting in the new value of r_1' through r_6' respectively, which fall in the nearly total transparency range of 238 through 254 in the alpha channel plane E_α .

Step 8 Embedding two fractional shares in the current block: Take block B_α in E_α corresponding to B_b in E_b select the first two pixels in B_α in the raster scan order and replace their values by r_1' and r_2' respectively.

Step 9 Embedding remaining partial shares at random pixels: the key K is used to select four pixels E_α but outside of the B_α . Whenever selecting these four pixels choose any pixels of block but not the first two pixels.

Step10 End of loop: If any un processed block is exists in E_b, then move for step 3. Otherwise take the E in the PNG format.

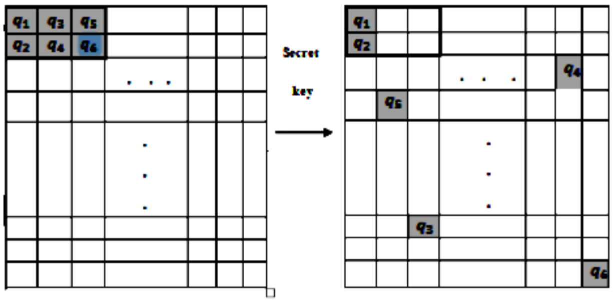


Fig 3. Pictorial representation of embedding 6 shares generated for a block, 2 Shares embedded in current block and the other 4 in 4 randomly selected pixels outside the block, with each selected pixel not being the first 2 one in any block

II. Algorithm for Authentication of Stego-Image

For the authentication of stego-image a detailed algorithm is proposed here.

Input: stego-image, the Output of the previous procedure

Output: The output of this procedure is image $\mathrm{I}_{\mathrm{AUTH}}$ with marked tamper blocks.

Steps:

1. First verify if the image contains alpha channel or not. If it does not contains alpha channel then neglects the whole image as un-authentic and request for the re-transmission of original image
2. The major gray values of image Z1 and Z2 are obtained by apply the moment-preserving technique to image I. Z1 and Z2 represents binary value of 1 and 0. Then using the formula (1) and binarization method calculate the threshold and save the binarized image IBAuth
3. Then take the scan of un-processed blocks of size 2×4 with values $p_1, p_2, p_3, \cdots p_6$ from the image IBAuth.

4. To form an 8-digit string, consider the values $p_1, p_2, p_3, \cdots p_6$ with the values 0's and 1's

5. Then this 8-digit string divided into two 4 digit strings represented as M1 and M2 and obtains the decimal equivalent of these numbers.

6. By using the *Shamir scheme* [11], and using the two secret values as M1 and M2, find out two shares along with K=2 as explained by the formula (2).

7. Then with the alpha channel values of the stego-image these two values are compared in the same block with the first column of block.

8. If any match happens then mark that block as authenticated and proceed to the next one.

9. Otherwise (if no mark), Mark the block as tampered and move to the next block.

10. After the completion of this entire process, all blocks are processed and we finally obtained the image as IAUTH.

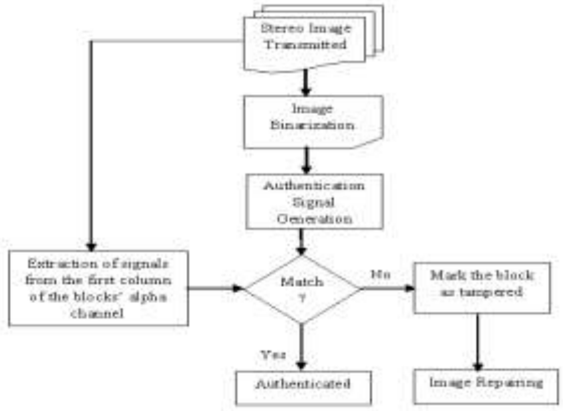

Stereo Image Transmitted
Image Binarization
Authentication Signal Generation
Extraction of signals from the first column of the blocks' alpha channel
Match ?
No
Mark the block as tampered
Yes
Authenticated
Image Repairing

Fig 4: flow chart for authentication of image

III. Algorithm for repairing of Image

Input: Authenticated image I.

Output: Image I_{REP} with the repaired pixels.

Steps:

1. To obtain the shares subtract 238 from the alpha channel.
2. Get the raster scan of block B of size 2×4 from I.
3. If not obtained, then move to the next block by marking this block as repaired.
4. If obtained, then choose 2 shares from the 6 shares which are preferably from a same block that are marked as un-tampered
5. Then the values M_1 and M_2 are obtained using the reverse Shamir Algorithm [12].
6. Then the values of M_1 and M_2 are converted into binary and these binary values are used to form 8-digit string
7. Transform the digits M_1 and M_2 into binary. Consider the each digit from the 8-bit string and transform them to gray value as follows
   a. If it is 0, then replace the corresponding pixel in the block of the image by Z2
   b) If it is 1, replace the corresponding pixel in the block of the image by Z1.
8. Proceed to the next block till the complete image is processed

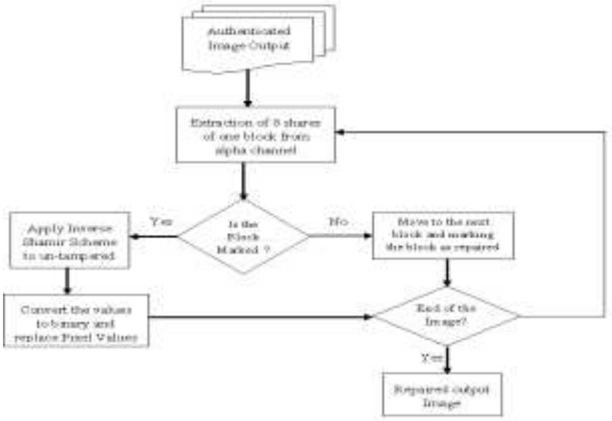

Authenticated Image Output
Extraction of 8 shares of one block from alpha channel
Is the Block Marked ?
Yes
No
Apply Inverse Shamir Scheme to un-tampered
Move to the next block and marking the block as repaired
Convert the values to binary and replace Pixel Values
End of the Image?
Yes
Repaired output Image

Fig 5: flow chart for repairing of image

RESULTS AND DISCUSSION

Fig. 6 original image

The image Lena, shown in Figure 6, is a 256 pixel width, 256 pixel height and 8-bits gray image. The value of each pixel is an integer between 0 and 255.

We use a □ □ 8, 4secret image sharing scheme, where t=4 and n= 8. By using the secret image sharing scheme described, we generate 8 shadow images which are shown in Figure 7. Since t=4 and the size of original image is 512X 512, the size of each shadow image is 128X 128. Since we use the □ □ 8, 4 secret image sharing scheme, we can use any four combinations of shadow images in the Figure 8 to get recovered image. The recover image is shown in Figure 8. By comparing with the original image, there is no error between the original image and the recovered image.

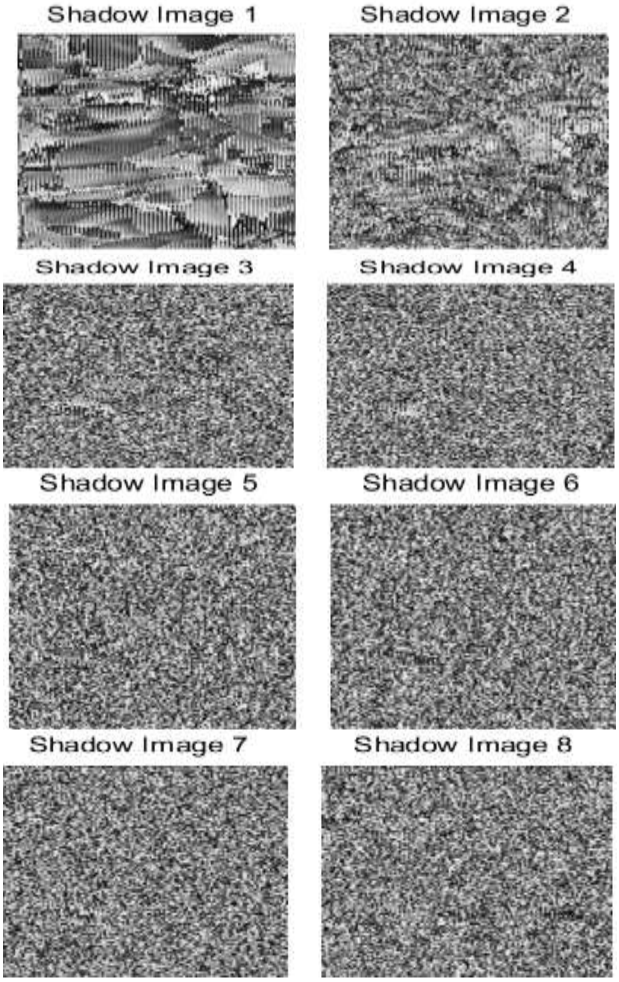


Fig 7: The 8 shadow images.

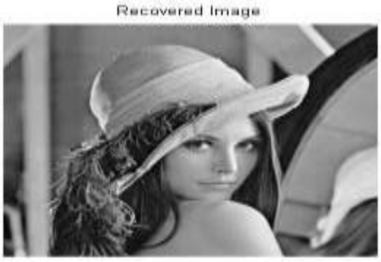
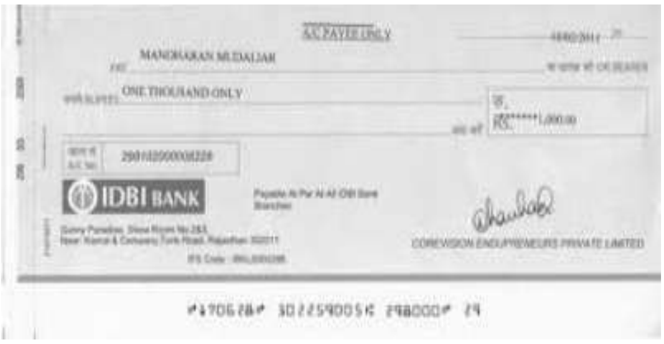


Fig. 8 recovered image



A/C PAYEE ONLY

MANOHARAN MUDALIAR

ONE THOUSAND ONLY

₹ RS. ******1,000.00

A/C No. 29810200000228

IDBI BANK

Payable At Par At All IDBI Bank Branches

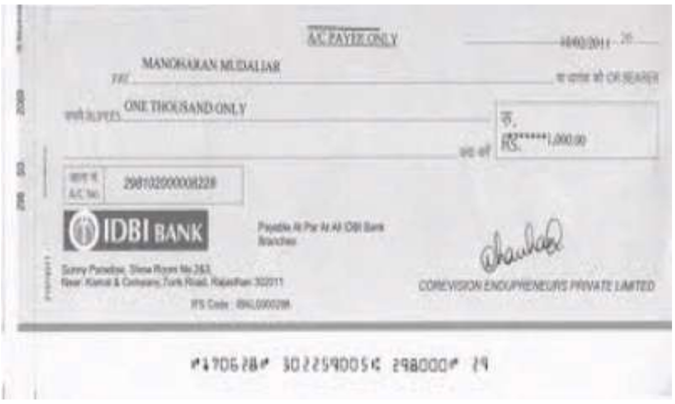
Sunny Paradise, Shree Room No 283,
Near Kamal & Company, Fork Road, Rajasthan 302011

IFS Code : IBKL000298

COREVISION ENDUPRENEURS PRIVATE LIMITED

⑈470628⑈ 302259005⑆ 298000⑈ 29

Fig. 9 Binary Gray scale image (input)



A/C PAYEE ONLY

MANOHARAN MUDALIAR

ONE THOUSAND ONLY

₹ RS. ******1,000.00

A/C No. 29810200000228

IDBI BANK

Payable At Par At All IDBI Bank Branches

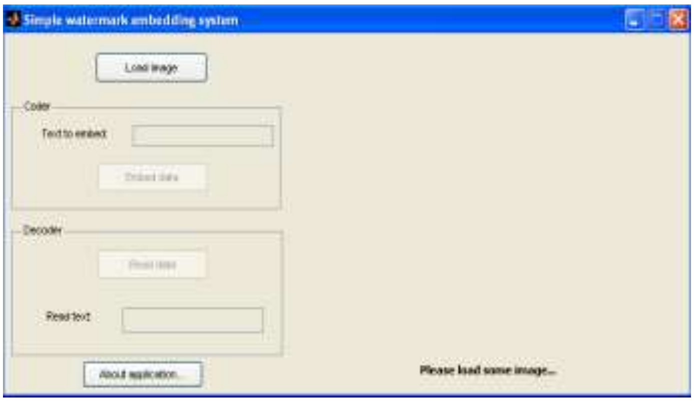
Sunny Paradise, Shree Room No 283,
Near Kamal & Company, Fork Road, Rajasthan 302011

IFS Code : IBKL000298

COREVISION ENDUPRENEURS PRIVATE LIMITED

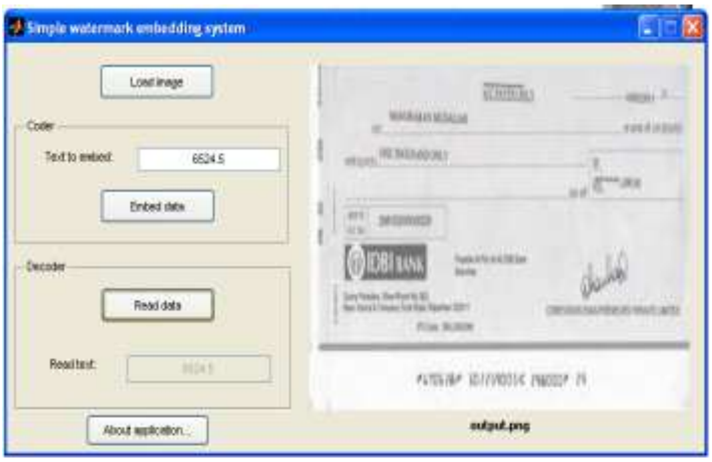
⑈470628⑈ 302259005⑆ 298000⑈ 29

Fig. 10 PNG image (output)



Please load some image...

Fig. 11 Binary Gray scale image (input)



Text to embed: 6524.5

Read text: 6524.5

output.png

Fig. 12 PNG image (output)

As shown in fig. 12 input image along with secret key is provided. To generate *n* secret shares by using *Shamir's secret sharing scheme* , E_b is used as input. Then the successfully mapped secret shares are combined with alpha channel plane to produce a PNG image with imperceptibility effect.

CONCLUSION

Shamir's Secret Sharing is an algorithm in cryptography. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret. Counting on all participants to combine together the secret might be impractical, and therefore we sometimes use the threshold scheme where any k of the parts is sufficient to reconstruct the original secret. Then using reverse Shamir scheme, two shares from unmarked blocks are collected and then data repairing is applied.

.

REFERENCES

[1] M. U. Celik, G. Sharma, E. Saber, and A.M. Tekalp, "Hierarchical watermarking for secure image authentication with localization," *IEEE Trans. Image Processing*, vol.11, no.6, pp.585-595, june.2002.

[2] C Yu, X Zhang "Watermark embedding in binary images for authentication", *IEEE Trans. Signal Processing*, vol.01, no.07, pp.865-868, September. 2004.

[3] A. Shamir, "How to share a secret," *Commun.ACM*, vol.22, no.11, pp.612-613, Nov, 1979.

[4] P.Jhansi Rani, S. DurgaBhavani1*stInt'1Conf on Recent Advances in Information Technology* RAIT-2012.

[5] Chih-HsuanTzeng and Wen-Hsiang Tsai, "A new approach to authentication of Binary image for multimedia communication with distortion reduction and security enhancement. *IEEE communication letters* VOL.7.NO.9 2003

[6] H. Yang and A. C. Kot, "Binary image authentication with tampering localization by embedding cryptographic signature and block identifier," IEEE Signal Processing Letters, vol. 13.

[7] M. Wu and B. Liu, "Data hiding in binary images for authentication and annotation," *IEEE Trans.on Multimedia*, vol. 6, no. 4, pp. 528–538, Aug. 2004.

[8] Che- Wei Lee and Wen-Hsiang Tsai "A secret-sharing-based method for authentication of grayscale document images via the use of the png image with data repair capability" *IEEE Trans. Image Processing*., vol.21, no.1, january.2012.

[9] Niladri B. Puhan, Anthony T. S. Ho "Binary Document Image Watermarking for Secure Authentication Using Perceptual Modeling" *IEEE International Symposium on Signal Processing and Information Technology*2005.

[10] W.H. Tsai, "Moment-Preserving thresholding: a new approach." *Computer Vision, Graphics, and Image Processing*, vol. 29, no.3, pp.377-393, 1985.

BIODATA.

Nagababu Manne presently pursuing his M.Tech degree in Sir C.R.Reddy Engineering College, Affiliated to Andhra University, India. He was graduated from Swarnandhra College of Engineering & Technology with Electronics and Communication Engineering as specialization.

K.J.Silva Lorraine obtained her M.E with Communication Engineering as specialization from CBIT, Hyderabad in the year 2010. While she was pursuing, she stood first in the college and even received medal for her academic excellence. She also received certificates of academic excellence for her performance in B.Tech and M.E. Presently, she is working as an Assistant Professor in Sir C R Reddy College of Engineering, Eluru.