ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

Authentication of Grayscale Document Images with Data Repair Capability Using Shamir's Secret Method

Vrushali Chirmade[1], Prof. Dimple Chaudhari[2]

Master Student, Dept. of Electronics and Telecommunication, YTIET, Karjat, India [1]

Professor, M.E(Extc), Dept. of Electronics and Telecommunication, YTIET, Karjat, India[2]

ABSTRACT*:* Digital images are used to safeguard confidential & important information. But the problem is providing authentication, integrity and data security to these digital images. In existing techniques of security and authentication conventional watermarking schemes are used. In these techniques cryptography is the basic method adopted which has problem of tampering of information easily by hackers. Therefore in this paper a new efficient authentication method is proposed for grayscale document images using the Portable Network Graphics (PNG) image with data repair capability. In this concept an authentication signal is generated by each block of a grayscale document image and then, using Shamir secret sharing scheme, authentication signal and binarized block content is combined and transformed into number of shares and then combined into an alpha channel plane forming the PNG image. This layer together forms a stego image. This stego image is sent to the receiver for authentication. If the grayscale image is tampered at the receiving end we can then make use of reverse Shamir's secret method and repair the tampered image.

KEYWORDS: data repair, grayscale document image, Portable Network Graphics (PNG) image, secret sharing.

I.INTRODUCTION

Authentication of digital documents are used in a wide range of application areas such as legal documents, certificates along with important records such as fax insurance and personal data which is later digitized and stored. Due to increase in computerized technologies, it is now easy to manipulate digital images without causing noticeable changes, resulting into illegitimate tampering of over send images. It is suitable to design effective ways to solve this kind of image authentication problem, especially for images of the documents whose surety must be protected. Hence, detection of forged image is of prime concern.

Image processing is a technique that involves the analysis and manipulation of a digitized image, especially in order to improve its level of excellence. In this paper we make use of Shamir's secret algorithm for producing the authentication signal and generating several shares 'k'. In this epoch, with the use of strengthened technologies it is liable to change the contents of these digital images hence it is necessary to protect its hypothecation. In the case of binary document images, it isnot easy to validate because of its straightforward binary nature that leads to perceptible modifications after authentication signal are embedded in the image pixel. So in this paper we are proposing authentication of grayscale document images. Grayscale images are high resolution binary image hence it is also known as binary like gray scale image. Grayscale images alter the visual quality limitation of binary certificates. In this paper we are using a new technique for verification of document images with an appended self data repairing capability for fixing tampered image data. The input image is accepted as binary like grayscale image shown in fig. 1.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

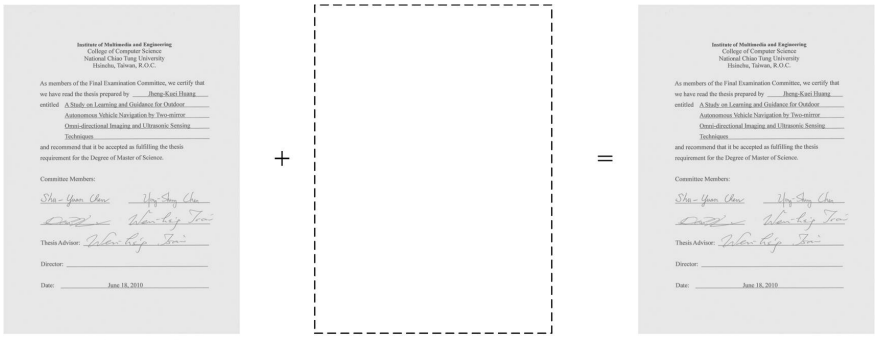
(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

Fig.1 Binary Gray Scale Image (Input)

After the proposed method is applied, the cover image is transformed into a stego-image in the Portable Network Graphics (PNG) format with an additional alpha channel for transmission on networks or archiving in databases as shown in fig. 2. The stego-image, when received or retrieved, may be verified by the proposed method for its

authenticity. Integrity modifications of the stego-image can be detected by the method at the block level and repaired at the pixel level. In case the alpha channel is totally removed from the stego-image, the entire resulting image is regarded as inauthentic.



grayscale document image (grayscale channel plane) | alpha channel plane | PNG image

Fig.2. Illustration of creating a PNG image from a grayscale document imageand an alpha channel.

II.RELATED WORK

REVIEW OF SHAMIRS SECRETSHARING METHOD

The proposed approach to secret image sharing is based on the (k,n)-threshold secret sharing method proposed by Shamir (1979). By the Shamir method, to generate n shares for a group of n secret sharing participants from a secret integer value y for the threshold k, we can use the following (k-1)-degree polynomial. 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 thethreshold 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.

ALGORITHMS FOR CREATING SHARES AND SECRET RECOVERY

1. Algorithm for Threshold secret sharing

Input: Secret d in the form of an integer, number of n participants and threshold $k \leq n$.
Output: n shares in the form of integers for then participants.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

i. Select a prime number p that is larger than d randomly.
ii. Select k -1 integer values c_1, c_2,…, c_{k-1} within the Range of 0 through p -1.
iii. Select n distinct real values x_1, x_2, x_3, …,x_n
iv. Use the following (k-1)-degree polynomial to compute n function values F(xi), called partial shares for i= 1, 2, …, n:

$$F(xi) = (d + c_1 x_i + c_2 x_i^2 + \cdots + c_{k-1} x_i^{k-1})_{mod\ p} \quad (1)$$

Send the two-tuple ((x_i, f(x_i)) as a share to the ith participant where i= 1, 2, .., n
There are k coefficients denoted d and c through, k shares are collected from n participants to form k equation to recover secret d.

2. Algorithm for secret recovery

Input: k shares collected from the n participants and the prime number p with both k and p being those used in Algorithm 1.
Output: secret hidden in the shares and coefficients used in (1) in Algorithm 1, where i= 1,2,3, ….k-1.

Steps.
Step 1: Use the shares (x_1, F(x_1),(x_2,F(x_2)),…..,(x_k,F(x_k)) to set up

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

Where j= 1,2,…k.

Step 2: Solve the k equations above by Lagrange'sinterpolation to obtain d as follows

$$d = (-1)^{k-1}\left[\begin{array}{l} F(x_1)\frac{x_2 x_3 \ldots x_k}{(x_1-x_2)(x_1-x_3)\ldots(x_1-x_k)} \\ +F(x_2)\frac{x_1 x_3 \ldots x_k}{(x_2-x_1)(x_2-x_3\ldots(x_2-x_k)} + \cdots \\ +F(x_k)\frac{x_1 x_2 \ldots x_{k-1}}{(x_k-x_1)(x_k-x_2)\ldots(x_k-x_{k-1})} \end{array}\right]_{mod\ p} \quad (3)$$

Step 3: Compute c1 through ck-1 by expanding the following equality and comparing the result with (2) in step 1while regarding variable x in the equality below to be x_j in (2)

$$F(x) = (-1)^{k-1}\left[\begin{array}{l} F(x_1)\frac{(x-x_2)(x-x_3)\ldots(x-x_k)}{(x_1-x_2)(x_1-x_3\ldots(x_1-x_k)} \\ +F(x_2)\frac{(x-x_1)(x-x_3)\ldots(x-x_k)}{(x_2-x_1)(x_2-x_3)\ldots(x_2-x_k)} + \cdots \\ +F(x_k)\frac{(x-x_1)(x-x_2)\ldots(x-x_{k-1})}{(x_k-x_1)(x_k-x_2)\ldots(x_k-x_{k-1})} \end{array}\right]_{mod\ p} \quad (4)$$

In the step 3 above algorithm is additionally included for the purpose of computing the values of parameters c_i in the proposed method.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

III.PROPOSED SYSTEM AND FLOW CHARTS

A. ALGORITHM FOR GENERATION OF STEGO IMAGE

A detailed algorithm for describing the generation of a stego image in the PNG format of the proposed method is presented in the following and illustration is shown by a block diagram in Fig. 4.

Stage 1: Generation of Authentication Signal

Step1:Binarization of input image: To get the two representative gray values g1 and g2, the Moment preserving threshold [3] is applied to I. The required threshold value is obtainedby averaging the g1 and g2. Using this threshold binary version of $I_b$will be obtained.

Step 2: Conversion of cover image into PNG format: By using alpha channel plane Iα the image I is converted into PNG image. This PNG image is created with 100% opacity and no colour as Iα.

Step3: Starting of loop: Take in a un- refined raster scan order of 2×3 block Bb in $I_b$with pixels p1, p2 , p 3, p4, p5, p6.

Step 4: Authentication signal generation: here generate a 2-bitauthentication signal s= a1a2with a1 = p1 ⊕p 2⊕p 3anda2= p4⊕p 5⊕p6.

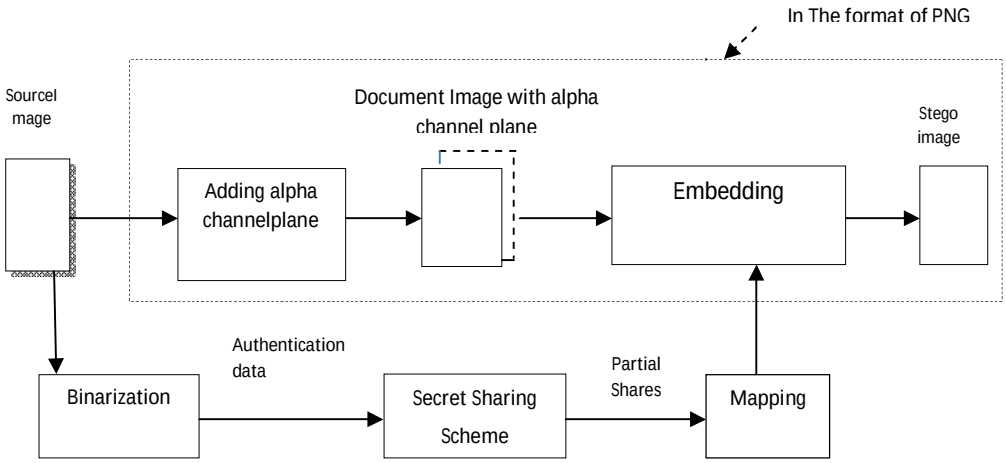


Fig.3 Illustration of creating PNG image from a grayscale document image and an alpha channel

Stage 2 : Design and Embedding of Shares

Step5: (Creation of data for secret sharing)In this step the datais created for secret sharing. Here the total 8 bits ofa1, a2and p1, p2, p3, p4, p5, p6forms an 8-bit string and this string is divided into two 4-bit segments, and finally convert the each segment into 2 decimal numbers m1 and m2 respectively.

Step 6:(Generation of partial shares) Set p, ci, xi of algorithm 1to be the following values(1) p=17 (the smallest Prime number larger than 15), (2) d = m1 and c1= m2 ; and 3) x1 = 1, x2 = 2,……x6 = 6. Using equation 1 and threshold secret sharing scheme and generate six partial shares q1to q6 using the following equations.

$$qi = F(xi) = (d+c1xi) \bmod p \qquad \text{where } i = 1,2,3,..6 \qquad (5)$$

Step7: (Mapping of the partial shares) Add 238 to each of q1through q6, resulting in the new values of q1' through q6', respectively, which fall in the nearly total transparency range of 238 through 254 in the alpha channel plane Iα.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

Step 8: *(*Embedding two partial shares in current block) Take block Bα inIα B_b corresponding to Bb in I_b , select the first two pixels in Bαin the raster-scan order, and replace their values by q1' and q2', respectively.
Step9:(Embedding remainingpartialshares at random pixels)Use key K to select randomly two pixels in Iα but outside Bα, which are unselected in this step, and not first two pixels of any block; in raster scan order; replace the four pixels by remaining partial shares q3' to q6' generated above respectively as shown in Fig. 3.

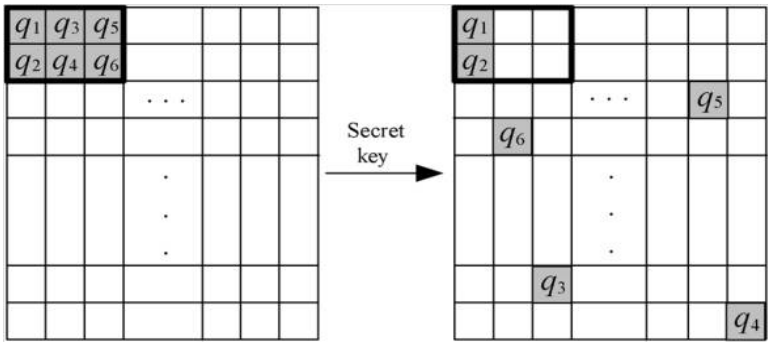


Fig.4Illustration of embedding six shares created for a block(steps 8 and 9 of algorithm A stage 2)

Two shares embedded at the current block, and the other four in four randomly selected pixels outside the block, with each selected pixel not being the first two ones in any block.

Step 10. (End of looping) If there exists any unprocessed block in Ib, then go to Step 3; otherwise, take the final in the PNG format as the desired stego-image I'.

Encrypt the PNG, take the final I in PNG with encrypted format as the desired stego-image I′. The prime number p used here is 17, so the values of q1 through q6 yield by equation (3) are between 0 and 16. After executing step 7 of above algorithm, they become q1′ through q6′ respectively which all fall into the small interval of integers ranging from 238 to 254 with a width of 17 (the value of the prime number). Consequent embedding of q1′ through q6′ in a narrow interval into the alpha channel plane means that very alike values will appear everywhere in the plane, resulting in a nearly uniform transparency effect, which will not stimulate notice from an attacker. We choose prime number to be 17 in the above algorithm because, if it was chosen instead to be larger than 17, then the above mentioned interval will be enlarged and the values of q1′ through q6′ will become possibly smaller than 238, creating visually whiter stego image. In contrast, the 8 bits mentioned in steps 5 and 6 above are transformed into two decimal numbers m1 and m_2 with their maximum values being 15(step 5 above) , which are forced to lie in the range of 0 through p-1 (step 2 in algorithm 1). Therefore p should not be chosen to be smaller than 16, i.e.; p=17 is the best possible answer.

B. ALGORITHM FOR STEGO IMAGE AUTHENTICATION

Input: stego-imageI' , the representative gray values g1 and g2 and the secret key K used in algorithm A.
Output: image Irwith tampered blocks marked and their data repaired if possible.

Stage 1—extraction of the embedded two representative gray values.
Step 1. (Binarization of the stego-image) Compute t=(g1+g2)/2, and use it as a threshold to binarize I' ,yielding a binary versionI_b' of I' with "0" representing g1 and"1" representing g2 .

Stage 2—verification of the stego-image.
Step 2. (Beginning of looping) Take in a raster-scan order anunprocessed block B' fromI_b' with pixel values p1 through p6 and find the six pixels values q1' through q6' of thecorresponding B'α block in the alpha channel plane I'α of I' .

Step 3. (Extraction of the hidden authentication signal)Perform the following steps to extract the hidden 2-bit authentication signal from s= s1s2 from B'α.
(1) Subtract 238 from each of q1' and q2' to obtain two partial shares q1 and q2 ofB'_b , respectively.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

(2) With shares and as input (1,q1), (2,q2) perform Algorithm 2 (Algorithm for secret recovery) to extract the two values d and c1 (the secret and the first coefficient value, respectively) as output.
(3) Transform d and c1 into two 4-bit binary values, concatenate them to form an 8-bit string , and take the first 2 bits a1 and a2 of S to compose the hidden authentication signal s=a1a2.

Step 4. (Computation of the authentication signal from then current block content) Compute a 2-bit authentication signal s'=a1'a2' from values p1 through p6 of B_b' the six pixels of by a1'= p1 ⊕p 2⊕p 3 and a2'=p4⊕p 5⊕p 6

Step 5. (Matching of the hidden and computed authentication signals and marking of tampered blocks) Match s and s' bychecking if a1=a1' and , and a2=a2' if any mismatch occurs,mark B_b' , the corresponding block B' in I' , and all the partialshares embedded in Bα' as tampered.

Step 6.(End of looping) If there exists any unprocessed block inIb' , then go to Step 2 in this algorithm; otherwise, continue.

The flow chart of above image authentication process is as shown in following Fig.

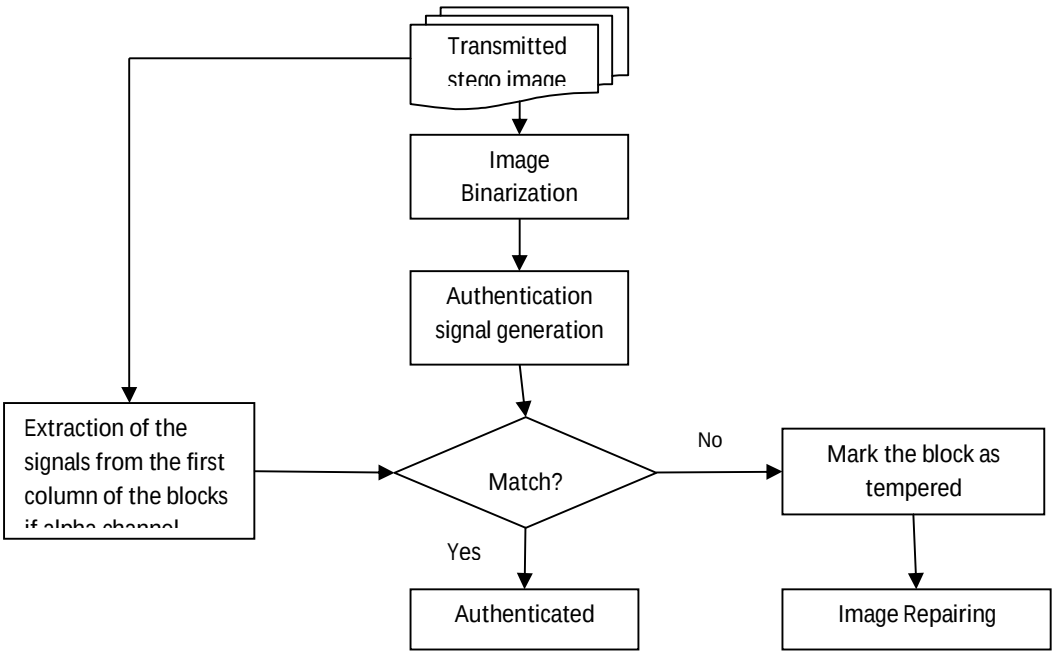


Fig 5. Flowchart for image authentication

Stage 3—self-repairing of the original image content
Step 7. (Extraction of the remaining partial shares) For each block Bα' in Iα' , perform the following steps to extract the remaining four partial shares q1 through q6 of the corresponding block B_b' in I_b' from blocks in Iα' other than Bα' .
(1) Use key K to collect the four pixels Iα' in the same order as they were randomly selected for B_b' in Step 9 of Algorithm A, and take out the respective data q3', q4' ,q5' and q6' embedded in them.
(2) Subtract 238 from each of q3' through q6' to obtain q3 through q6 , respectively.

Step 8.(Repairing the tampered regions) For each block B' in I' marked as tampered previously, perform the following steps to repair it if possible.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

(1) From the six partial shares q1 through q6 of block B_b' in I_b' corresponding to B' (two computed in Step 3(1) and four in Step 7(2) above), choose two of them, e.g. qk and ql which are not marked as tampered, if possible.
(2) With shares (k, qk) and (l, ql) as input, perform Algorithm 2 to extract the values of d and c1 (the secret and the first coefficient value, respectively) as output.
(3) Transform d and c1 into two 4-bit binary values, and concatenate them to form an 8-bit string S'.
(4) Take the last 6 bits from b1', b2', ... b6' from S' , and check their binary values to repair the corresponding tampered pixel values y1', y2', …, y6' of block B' by the following way: if bi'=0, set yi' =g1 ; otherwise, set yi' = g2 where i 1, 2, .., 6.

Step 9. Take the final I' as the desired self-repaired image Ir.

The complete process of repairing the image is shown in flowchart that is Fig. 6

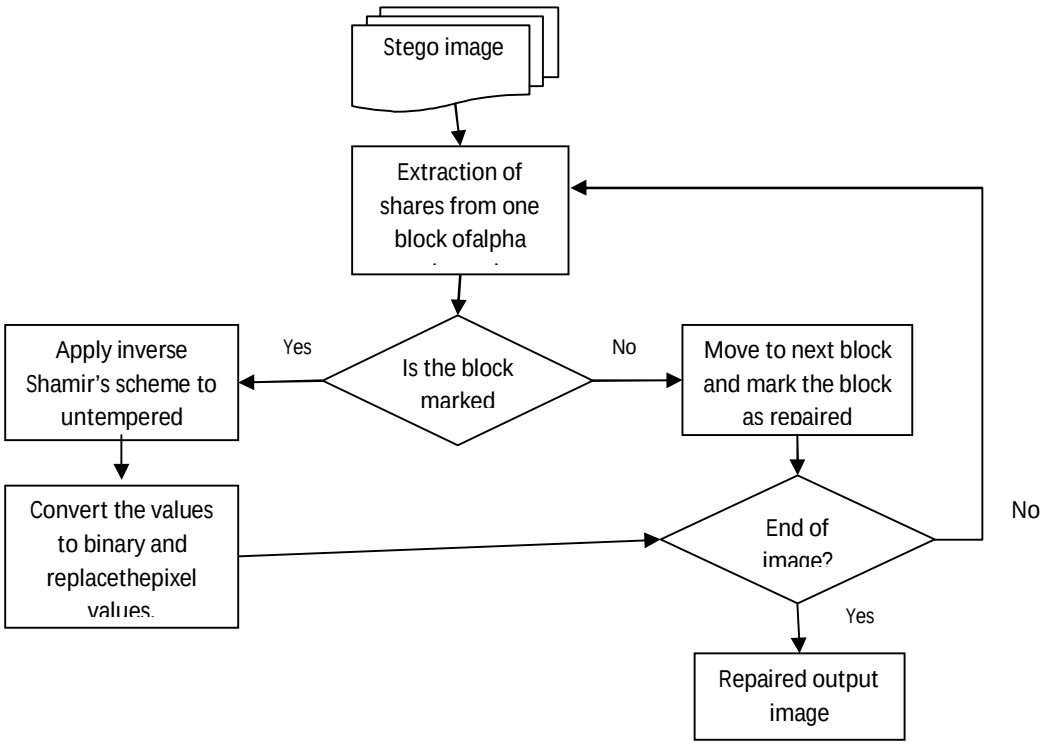


Fig. 6 Flowchart for repairing of the image

IV.SIMULATION AND RESULT

Now, For simulation we have taken one sample document image. The image is processed and stego image is obtained. In image 1 input image, Threshold image, PNG image and stego image obtained by processing are shown.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

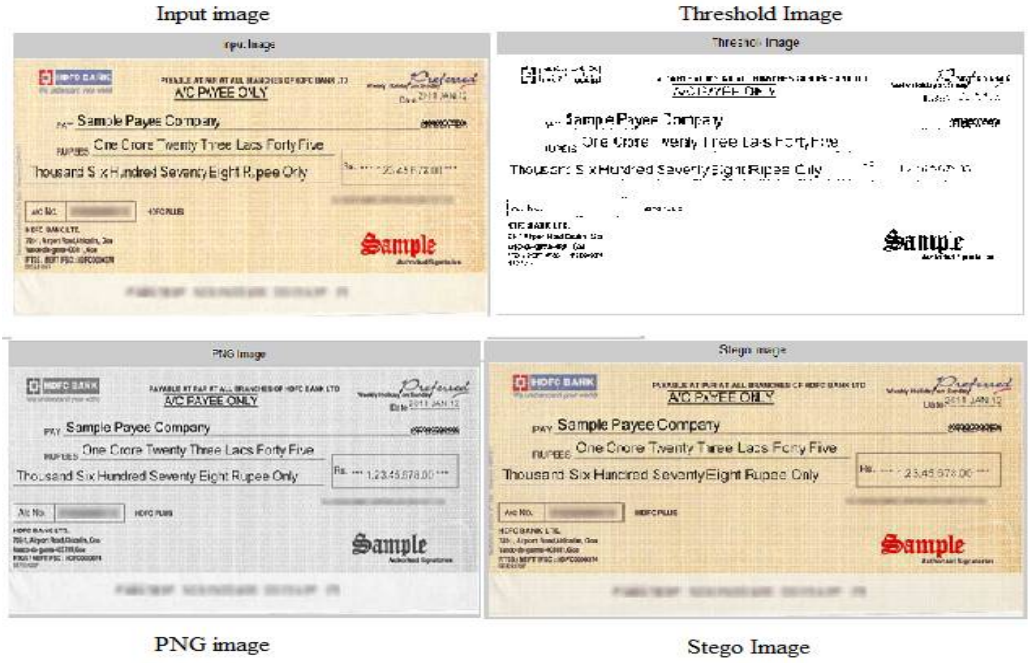


Image 1.simulation results for generation of stego image

Now, Two common operations are usedfor editing the image. They are superimposing and painting. The superimposing operation destroys the content of the alpha channel values. It replaces all the original alpha channel values at the attacked part with the new values of 255. By following Image 2 we can see that original grayscale image is extracted from edited one.

Image 2. Simulation results for reparing of tempered image

We have seen complete process of grayscale image authentication and reparing by algorithm and flowcharts fig. 5 and fig 6 and by simulation results images Image 1 and Image2.

V. CONCLUSION

We have proposed a secure authentication scheme for grayscale document images by the use of secret sharing method. In this scheme security is provided by, secret sharing and encryption. Using Shamir secret sharing method both the generated authentication signal and the content of a block are transformed into partial shares. Which are then distributed in an elegant manner into an alpha channel plane to create a PNG image.This image is encryptedand a stego image is formed. In the authentication process, if it seen that the data is tampered then self-repairing is done in the content of the tampered block by reverse Shamir scheme. This method enhances the security by embedding the data in the alpha channel plane and encrypting the PNG image. Future studies may be directed to choices of other blocksizes

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

and related parameters (prime number, coefficients for secret sharing, number of authentication signal bits, etc.) to improve data repair effects.

REFERENCES

[1] Shamir, Adi (1979), "How to share a secret", Communications of the ACM
[2] 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 a Data Repair Capability", Student Member, IEEE, , Senior Member, IEEE, January 2012.
[3] Authentication of Grayscale Document Images by using PNG Image with a Data Repair Capability T.M.Prasanth1, K.Jansi Lakshmi2, (DSCE) Student, 2Assistant Professor, 3Associate Professor & Head Department of ECE, AITS -2278-5140, Volume-2, Issue – 2, 2013-IJACECT
[4] Authentication of grayscale document images using Shamir secret sharing scheme.1.Mrs.G.Niranjana,M.Tech(Asst.prof), 2. Ms.K.SivaShalini,M.Tech .International Journal of Computer Trends and Technology (IJCTT) – volume 5 number 1 –Nov 2013.
[5] A.C. Kot and H. Yang, "Pattern-based data hiding for binary images authentication by connectivity preserving," IEEE Trans. Multimedia, vol. 9, no. 3, pp.475–486, Apr. 2007.
[7] B. Liu and M. Wu, "Data hiding in binary images for authentication and annotation," IEEE Trans. Multimedia,vol. 6, no. 4, pp. 528–538, Aug. 2004.
[8] W.H.Tsai and C.H.Tzeng, "A new approach to authentication of binary images for multimedia communication with distortion reduction and security enhancement," IEEE Communication. Lett. vol. 7, no. 9, pp. 443–445, Sep. 2003.
[9] 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.