INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 06, June 2024, pp: 1524-1530

e-ISSN : 2583-1062

Impact Factor: 5.725

MONOCHROME IMAGE AUTHENTICATION WITH DATA REPAIR CAPABILITY

Darshan Thakur[1], Neharkar Savita[2]

[1]Lecturer, Electronics and Tele. Engineering Department, Terna Engineering college, Dharashiv, Maharashtra, India.

[2]Lecturer, Electronics and Tele. Engineering Department, Swami Vivekanand Polytechnic, Kaij, Maharashtra, India.

ABSTRACT

The technique of image authentication has become increasingly popular in recent years. The digital revolution in image processing has made it feasible to quickly and easily create, manipulate, and transport digital images. Therefore most of the vital photos such as military, Medical, Companies secret data must be protected against alteration. So to safeguard originality and validity of multimedia images and essential scanned documents many authentication methods are evolved. The usage of portable network graphics (PNG) images with bitplane slicing method in this study provides an image authentication scheme with data repair capability. Experiments indicate that the authentication system can withstand and repair original data in the face of various attacks. It also demonstrates the work's effectiveness.

Keywords - Authentication, Fragile Watermarking, Semi Fragile watermarking, Tamper Detection.

1. INTRODUCTION

Due to the advent of advanced image editing tools, the saying "the photograph doesn't lie" is no longer accurate. Because of their ease of manipulation, processing, and storage, digital photographs have become popular. It's nearly hard to tell which photographs are genuine and which have been modified on a subjective level. The credibility that photography used to have has been eroded as a result of technological advancements. At every level of transmission and storage, image authentication algorithms safeguard images from malicious alteration. Image authentication system that is reliable must be able to protect an image from the time it is created until it is used. A digital image is a method of archiving vital data. With the rapid advancement of digital technologies, it is now possible to make virtually undetectable changes to the contents of digital photos. As a result, ensuring the integrity and authenticity of a digital image is a difficult task. Effective approaches for solving this type of image authentication problem [1]–[2] are desirable, especially for photos of documents whose security must be preserved. It's also intended that if a portion of a document image is found to have been tampered with, the damaged content can be restored. These image content authentication and self-repair capabilities are useful for the security protection of digital documents in a variety of fields, including important certificates, important signed digital images, signed documents, scanned cheques, circuit diagrams, art drawings, design draughts, and last will and testaments, among others. Authenticity is a relative concept in general: whether or not an object is authentic depends on a reference or a specific sort of representation that is considered authentic. Authentication is typically accomplished by determining if certain rules and relationships that are expected to be present in an authentic copy are still present in the test material. Following is the basic image authentication algorithm with data repaircapability.

If (Received watermark ~ = Original Watermark)Statement = Manipulation Occurs.

else

Statement = Manipulation Not occurs.

end

2. METHODOLOGY

This describes the overview of the system that is developed. The Grayscale image authentication with data repair capability is proposed. This containsthe authentication data embedding and authentication checking algorithms. The proposed technique first convert input grayscale image into Portable network graphics (PNG) format by adding alpha channel. At the same time binarization of data for authentication and repairing is done. This data is embedded into alpha channel by keeping transparency at highest level. Stego image is generated in PNG format. Following steps are involved in the authentic data embedding process. Fig 2. shows the details of authentic data embedding process

A.Stego Image Formation

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 06, June 2024, pp: 1524-1530

Step 1: Cover Image

The input grayscale image is an 8 bit image. That grayscale image we can use for embedding authentic data. The input grayscale image has an extension of PNG, JPG, BMP, etc. The input grayscale image represented using following expression. Let A be an input grayscale image having size $m * n$ andrepresented as:

A= { (i, j) | 1 ≤ i ≤ m, 1 ≤ j ≤ n }

(i, j)c {0,1,2,3,4,.....,255}

Step 2: Alpha Channel Addition

The alpha channel will cause unpredictable transparency in the final PNG image, resulting in an opaque look that is undesired. One solution is to translate the resulting alpha channel values into a tiny range near 255, resulting in an almost undetectable transparency effect on the alpha channel plane. The alpha channel is described in the following way. 1 ≤ i ≤ m, 1 ≤ j ≤ n $Alpha$ = { (i, j) | x(i, j) = 255 } The alpha channel used as a carrier for embedding authentic data. At the same time transparency of the image is also maintained by alpha channel.

Algorithm 1: Preparation of the cover image i.e.Creation of PNG image
Input: Select Cover Image
Output: Modified cover image.png

Step 1: Select cover image
if (cover image is PNG)
{
There is no need to add alpha channel
}
else
{
Add alpha channel to form PNG image
}
Step 2: End

Step 3: Binarization and mapping of authentic data for embedding purpose.

In this step Binarization of cover image is done. For Binarization of cover image for embedding purpose bitplane slicing is used and using bitplane replacement embedding operation is done in cover image. For grayscale images have 8 bit-planes, this can be represented as follows:

Plk 1 ≤ i ≤ r, 1 ≤ j ≤ c = {(i, j, k)| x(i, j, k) c {0,1} } … … Where: 1 ≤

k ≤ 8 Input cover image is a grayscale image has 8 bits/pixels. It also has 8 biplanes.

Algorithm 2: Binarization (Bitplane slicing)
Input: Cover Image
Output: 8 bitplanes of cover image

Step 1: Select cover image

Step 2: Slice the cover image into 8 bitplanes

1 ≤ i ≤ r, 1 ≤ j ≤

Plk = {x i, j, k | }

(i, j, k) c {0,1}

W$here$: 1 ≤ k ≤ 8 (i, j, k) c {0,1. Pl1, Pl2, Pl3, Pl4, Pl5, Pl6, Pl7 and Pl8

Step 3: For embedding purpose

we only select Pl4, Pl5, Pl6, Pl7 and Pl8 because these bitplanes has highest information as compared with other bitplanes.

Step 4: End

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 06, June 2024, pp: 1524-1530

Step 4: Mapping and Embedding

This is the most important step in the whole process. In this step bitplane 4,5,6,7,8 are embedded into alpha channel and alpha channel will combined with grayscale image. Figure 4.6 shows a clear image about embedding of authentic data in alpha channel. While embedding authentic data inalpha channel we only consider bitplane number 4 to bitplane number 8. Bitplane number 4 to 8 has highest information of the cover image. The size of alpha channel and size of the input grayscale image should be same.

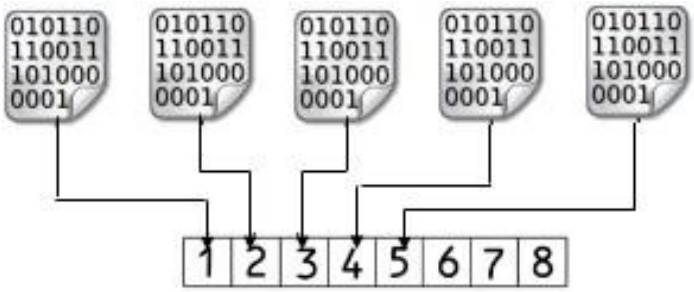


Fig 3. Replacing Alpha channel bitplanes with Authentic Data

1 st five bitplanes of alpha channel are replaced by authentic data to get final stego alpha channel. The following algorithm 3 is about formation of stego alpha channel. In this algorithm embedding of bitplanes in alpha channel is done

Algorithm 3: **Mapping and Embedding bitplanes in alpha channel**
Input: Alpha Channel and bitplanes $Pl1$
Input: Alpha Channel and bitplanes $Pl1$

Step 1: Take Alpha Channel (the size of alpha channel and cover grayscale image should be same) Step 2: Take $Pl4$, $Pl5$, $Pl6$, $Pl7$ *and* $Pl8$ from slicing of grayscale image

$1 \leq i \leq r$, $1 \leq j \leq$ ◆

$Plk = \{(i, j, k) | x(i, j, k) \text{ c } \{0,1\} \}$

Step 5: Formation of stego Monochromatic image

Final stage of this process is of forming stego grayscale image. The stego alpha channel is combined with the input cover image for getting stego grayscale image. Algorithm 4 is about combining stego alpha channel with cover image. The output of this algorithm is stego grayscale image.

Algorithm 4: Forming Stego Monochromatic Image
Input: Cover Image and Stego alphaChannel
Output: Stego Grayscale Image S
Step 1: Take Cover Image and Stego alpha channel Step 2: Combine cover image and stego alpha channel together Step 3: Stego Grayscale Image S= Cover Image + Stego Alpha Channel Step 4: End

3. MODELING AND ANALYSIS

This includes stego image verification and self-repairing process. In this process first authentic data is extracted from stego image and it is matched with the computed authentication data. If both data's are matched with each other then it is authentic image. If it is not matched then it is not authentic data. If second case occurs then move for further processes of verification and self-repair. The stego image authentication includes three important

The stego image authentication includes three important stages.

Stage 1: Extraction of authentic data from alpha channel

Stage 2: Verification of the stego image

Stage 3: Self repairing of original image content.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 06, June 2024, pp: 1524-1530

Figure 4 shows all three stages in detail. Stage 1 is about extraction of authentic data from alpha channel. Stage 2 is about verification of stego image and stege 3 is about self- recovery of original image content.

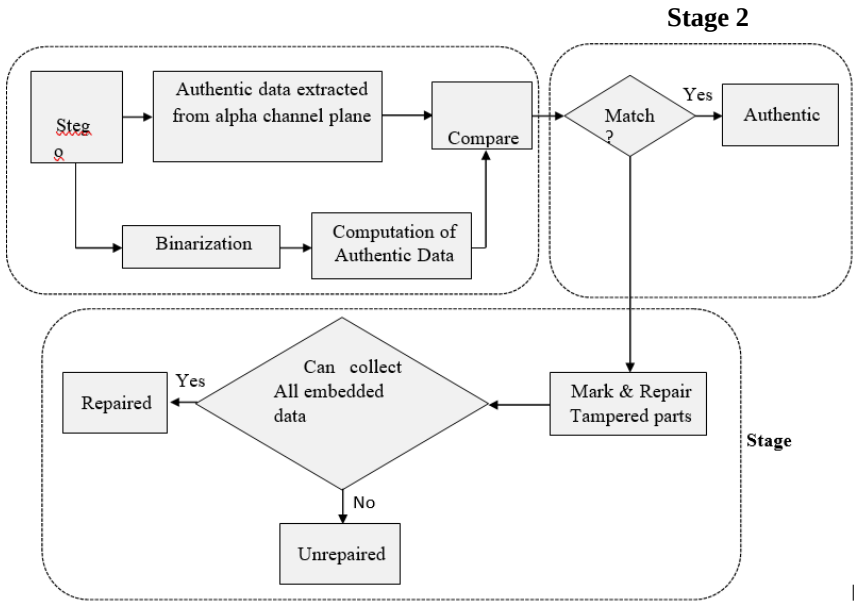


Fig 4. Authentication process including verification and self-repairing of a stego Monochromatic image in PNG format.

4. RESULTS AND DISCUSSION

In this, simulation results are given to demonstrate the performance of the Developed algorithms. The main idea of these algorithm is to find image or scanned document is authentic or not and if it not authentic then find alteration mode and repair tampered data. The main objectives of developing these algorithms are to embed authentication data with host file not in the separate file, to tampered area on image, to repair original content of tampered area and keep visual quality of image high after embedding authentication data in host file. Different types of objective parameters are used to analyze quality of the stego image and quality of the repaired image. Objective image quality assessment (IQA) comprises two categories one is full reference IQA and second is No reference IQA. For analyzing above algorithm parameters from full reference IQA have been chosen. The following parameters are used from FR-IQA for analyzing quality of the stego and repaired image. Mean Square Error (MSE), Peak-Signal to Noise Ratio (PSNR), Normalized Cross Correlation (NCC), Average Difference (AD), Structural content (SC). Two more parameters are defined specifically for analyzing developed algorithms are Embedding capacity (EC), Number of bits embedded (NBE). The results are taken for different images like grayscale image, Grayscale document image, color image and color document image. This algorithm is also tested for criminal face authentication. Algorithm can take any size of image. There is no restriction for image size. The results are taken in following sequence. 1. First authentication data is embedded into the alpha channel 2. Various quality parameters are recorded in a table 3. Different attacks are applied over a stego image 4. Attacked image is repaired and quality parameters are recorded. Results for Monochromatic image authentication A. Authentication Data embedding The standard Lena image is taken as a cover image. The size of the image is 512*512

(a) (b) (c)

Fig 5 Authentication Data Embedding Process of Monochromatic Image (a) Cover Image (b) Alpha Channel + Authentication Data (c) Stego image

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 06, June 2024, pp: 1524-1530

The quality parameters for above embedding process is listed below. The parameters consist of PSNR, MSE, SC, NCC, AD, EC and NBE.

IMAGE QUALITY PARAMETER VALUES FOR GRAYSCALE IMAGE

Image Quality Parametergrayscale image	Values
PSNR in dB of Grayscale Image	100
PSNR in dB of Alpha Channel	22.7994
MSE of Alpha Channel	338.634
SC of Alpha Channel	0.880012
AD of Alpha Channel	15.9625
NCC of Alpha Channel	1.06522
EC of Alpha Channel	2097152
NBE in Alpha Channel	1310720

B. External Attacks on Stego Image,

Authenticity verification and data recovery The images are attacked by several techniques. In this study we have focused on intentional attacks. Intentional attacks comprises following manipulation activities.

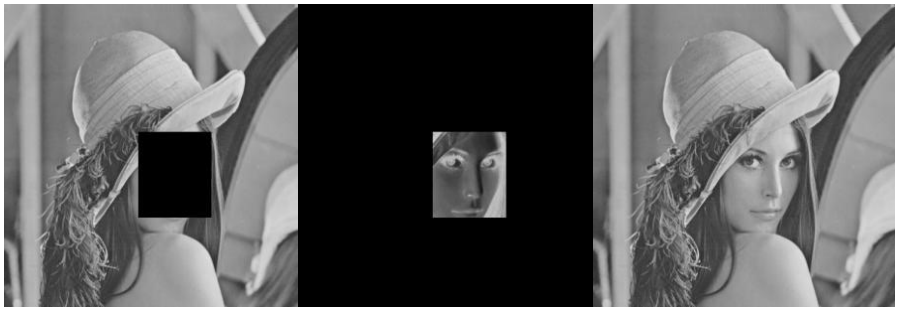
i)Image Cropping

ii) Text attack

Now algorithm 5 from chapter 4 is checked for all above attacks for authenticity verification and data recovery. 1) Image Cropping Attack, Authenticity verification and data recovery. The face is cropped to vanish the evidence. Fig 6 shows the cropped image.

Fig 6. Cropping attack on Monochromatic Image

Image cropping is applied on stego image to vanish the identity of image. Now authenticity verification and data recovery is applied over cropped image to recover original content of the lena image.



(a) (b) (c)

Fig 7. Authentication, verification and Data recovery of Monochromatic Image

(a) Subtraction of Authentication data and verification data (b) Tamperedarea identification (c) Repaired Image

Fig 7 shows detailed Authentication verification and Data recovery outputs. Fig 7 (a) is a subtraction of authentication data embedded into alpha channel and data extracted for verification from grayscale image. Figure 7 (b) is an identification of the tampered area and Figure 7 (c) is a repaired image. This image is obtained by mapping authentication data to tampered area.

The following quality parameters are recorded for checking quality of the repaired image. Quality checking is done between repaired image and input cover image. Following table 2 comprises all the quality parameters.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 06, June 2024, pp: 1524-1530

TABLE 2. REPAIRED IMAGE QUALITY PARAMETERS GRAYSCALE IMAGE FOR CROPPING ATTACK

Image Quality ParameterGrayscale Image	Values
PSNR in dB	46.7197
MSE	1.22589
NCC	1.00176
SC	0.99643
AD	0.245876

1. Text Attack, Authenticity verification and data recovery In this attack externally text is inserted on image to claim ownership of the image. Figure 5.4 shows the text attack.

Fig 8. Text attack on Monochromatic Image

Anyone can claim ownership of the image by inserting the text on image. In above Figure 8 @ARN text is inserted externally to claim the ownership of the image

(a) (b) (c)

Fig 9. Authentication, verification and Data recovery of Monochromatic Image

(a) Subtraction of Authentication data and verification data (b) Tampered area identification (c) Repaired Image

Figure 9 shows detailed Authentication verification and Data recovery outputs. Figure 9 (a) is a subtraction of authentication data embedded into alpha channel and data extracted for verification from grayscale image. Figure 9 (b) is an identification of the tampered area and Figure 9 (c) is a repaired image. This image is obtained by mapping authentication data to tampered area.

The following quality parameters are recorded for checking quality of the repaired image. Quality checking is done between repaired image and input cover image. Following table 5.3 comprises all the quality parameters.

TABLE. 3. REPAIRED IMAGE QUALITY PARAMETERS GRAYSCALE IMAGE FOR TEXT ATTACK

Image Quality ParameterGrayscale Image	Values
PSNR in dB	55.5631
MSE	0.159996
NCC	1.00017
SC	0.999651
AD	0.03228

5. CONCLUSION

The algorithms developed for authentication of grayscale and color images embeds authentication data in the host file rather than in a separate data file. If authentication data embeds in a separate data file and if it is lost due to manual mistakes then it's a huge loss. In this case no one can check whether given image is authentic or not. This embedding approach increase complexity at the authentication checking. The developed algorithms embeds authentication data in alpha channel not in the grayscale image pixel. This embedding approach in an alpha channel keeps grayscale image or color image pixels unchanged. The results shows the quality of the stego image after embedding authentication data is high. The developed algorithms embeds authentication data in an alpha channel. Alpha channel produces transparency effect to the image. Authentication data is embedded into the alpha by using bitplane slicing in the highest bitplanes to reduce the opaque effect visible in the stego-image. The opaque effect visible in the stego-image when authentication data embedded into the lower bitplanes of an alpha channel. There are only few techniques in the research which works for authentication and data recovery of grayscale image. Most of the techniques in the literature embeds binary like data to check authenticity and for recovery. The proposed techniques embed five bitplanes of grayscale image in an alpha channel. These five bitplanes has highest information of the grayscale image. At the time of authenticity checking and recovery, maximum grayscale data is repaired. The result shows the quality of repaired image is 90%.

6. REFERENCES

[1] Rafeal Gonzalez et al., "Digital image processing", 3 rd edition, published by Pearson India Education services Pvt Ltd, 2016.

[2] Anand, A., Raj, A., Kohli, R., & Bibhu, V., "Proposed symmetric key cryptography algorithm for data security", International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), pp. 159-162, 2016.

[3] Omar Farook Mohammad et al., "A Survey and Analysis of the Image Encryption Methods", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, pp. 13265- 13280, Number 23, 2017.

[4] H. B BasanthKumar, "Digital Image Watermarking: An Overview", Oriental Journal of Computer Science & Technology, Vol. 9, No. (1): pp. 07-11, April 2016.

[5] Naina Choubey and Mahendra Kumar Pandey, "Transform based Digital Image Watermarking: An Overview", International journal of Computer Trends and Technology (IJCTT), 24(2); pp. 80-83, 2015. [6] R. English, "Comparison of High Capacity Steganography Techniques ", IEEE, International Conference of Soft Computing and Pattern Recognition, pp.448-453, December 2010.

[6] H. Sajedi, and M. Jamzad, " Secure steganography based on embedding capacity ", Springer Verlag, International Journal of Information Security, Vol.8, Issue 6, pp.433-445, August 2009.

[7] T. Morkel, " Image Steganography Applications for Secure Communication ", M.Sc. thesis, Faculty of Engineering, Built Environment and Information Technology University of Pretoria, Pretoria, pp.126- 132, May 2012.

[8] Y. Lee, H. Kim, and Y. Park, "A new data hiding scheme for binary image authentication with small image distortion", Inf. Sci., vol. 179, no. 22, pp. 3866– 3884, Nov. 2009.

[9] H. Yang and A. C. Kot, "Pattern-based data hiding for binary images authentication by connectivitypreserving", IEEE Trans. Multimedia, vol. 9, no. 3, pp. 475–486, Apr. 2007