INTERNATIONAL RESEARCH JOURNAL ON ADVANCED SCIENCE HUB
e-ISSN : 2582 - 4376
Open Access
RSP SCIENCE HUB
(The Hub of Research Ideas)
Available online at www.rspsciencehub.com

Image Security using Self embedding Fragile Watermarking Method

Swapna.Enugula[1],Srujana.V [2], Karthik nasani[3],G.Shruthi[4],V.Vikram[5]
[1,2,3,4,5]Assistant Professor, ECE, Kamala Institute of Technology &Science, Singapur, Karimnagar, Telangana, India
eswapna.s@gmail.com[1]

Abstract

Rapid development in technology to provide security to data in the form of images is a major issue. So to provide security to the original image, watermark image embedded in it. In this paper we use self embedded watermark using fragile watermark technique. Authenticity of an image can be tested using block based technique of self embedding fragile watermarking; to represent the entire image the feature image watermark is used. In each 2x2non overlapping block four authentication bits and eight recovery bits are generated. In each block three least significant bits are embedded with authentication bits and recovery bits are embedded in the three least significant bits of the mapped block This paper mainly summarizes the Selection of image, method of watermark insertion, detection and tamper localization and recovery procedure. The experimental results of this proposed method shows visual quality of image recovery better than some of the schemes.

Keywords: Self embedding,, Block based fragile watermark , Authentication, Tamper recovery

1. Introduction

Presently digital image processing technology is highly diverse; the image content can be easily manipulated by unauthorized users. For legal cases replacement of content in an image is very harmful [1]. Therefore research on detection and localization of tampered images is an important issue. For this digital watermarking technique is widely used. In this technique of inserting secret information or image's information into an original image prior to sending. Confidential information is inserted in original image, while the secret information is a watermark [2–3].The watermark technique is used for component selection. In general watermark is used for image authentication and image recovery. In self embedded watermarking scheme the watermark is generated from the original image. Digital watermarking can be done by using several techniques like robust watermark, semi fragile watermarking and fragile watermarking. Fragile watermarking scheme can be categorized into two types for the authentication of an image. The two schemes are fragile watermark pixel wise scheme and fragile watermark bock wise scheme. In fragile watermark pixel wise scheme the watermark information is generated from the grey pixel value of the host image .In case of block wise watermark scheme, the original image is sub divided into blocks. For each sub block is authenticated with watermark information. The successful retrieving of the sub-block is difficult, if watermark image is modified. The fragile watermarking scheme also used for reversible data.

2. Principle of Operation

Now a day's self- embedding fragile watermarking scheme is used for the purpose of damaged image authentication and recovery. In this method image capture feature can be divided

into block-wise and pixel-wise mechanism .In block-wise algorithm to embed watermark in image the original image is divided into small blocks [1-6].For image tamper detection and recovery there are two stages of watermark algorithm they are watermark phase and authenticating phase.

Perceptibility: The embedded watermark is not visible, authorized persons can recover the high quality image from the watermarked image.

Tamper detection: To detect the secured data from the original image or derive some information from the image self fragile watermarking technique is used.

Tamper recovery: This technique is used to detect unauthorized modification on images and recover them from the tampered ones.

3. Mechanism of selection, generation and method of Insertion watermark

Based on the need for digital image recovery the watermark component is selected, thus the original image needs to be divided into the appropriate blocks, mapping the blocks before insertion by a specific method is shown in the fig1.

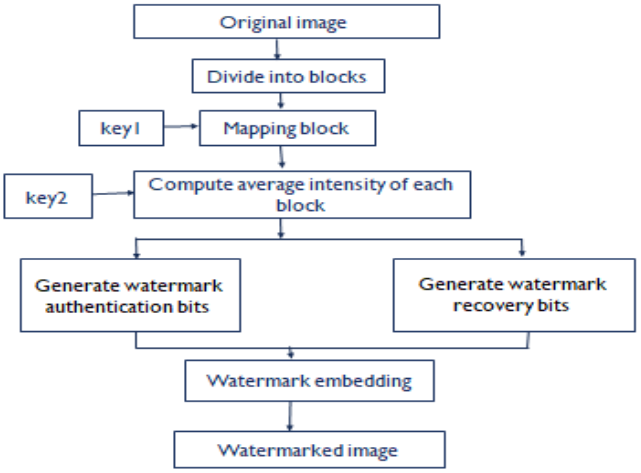


Fig. 1 Block diagram of watermark embedding

The original image is the image where the confidential information is inserted. Let us consider the original image be the image of Indian Navy Mission. Hidden image is a secret image which consists of confidential information that would be inserted as a watermark to the original image shown in fig 2.

3.1. Operations performed on original image and hidden image:

1. Initializing and reading the image.

Original image : 720 x 1280 x 3 uint8

Fig. 2 Original image

2.Getting the number of rows, columns and number of colour channels visible rows : 720
Visible columns : 1280
Number of colour channels : 3

3. Converting the original image into gray scale image and extracting any of the color from RGB.

Fig.3 original gray scaled starting image

4. Initializing and reading the image. Hidden image : 239x320x3 uint8

Fig. 4 Hidden image

5. Getting number of rows, columns and number of colour channels.

Hidden rows	:	239
Hidden columns	:	320
Number of colour channels	:	3

6.Converting the image into grey scale image and extracting any of the colours from RGB.

Fig. 5 Gray scaled Hidden image

7. Getting the histogram of the hidden image

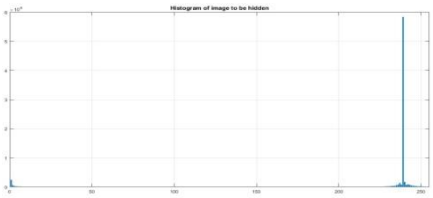


Fig. 6 Histogram of Hidden image

3.2 Procedure of Block wise segmentation:

In this procedure the original image is divided into blocks of uniform size (nxn pixels). So far they have investigated experiments with bocks of different size,i.e.,2x2 pixels[8], 3x3 pixels,4x4[9] pixels and 8x8 pixels. These blocks were used to generate more watermarks, as authentication and recovery bits. In 2016, a scheme using a small non-overlapping block sized 2x2 to improve the accuracy of localization and effectively remove the blocking artefacts as illustrated in the fig. 7

The original image X of size mxn is divided into non-overlapping blocks of size 2x2[8]. It was also stated that the small block sizes generally allow for better tamper detection. This also allows better block encoding when textured blocks are smooth. Meanwhile, to localize tamper the original image is divided into blocks of size 3x3. Xiao's method[9] divides an image into 4x4 non-overlapping blocks, generates the authentication watermarks for the bocks by comparison and parity check among average intensities and embeds them into corresponding blocks. The recovery information of another block is embedded into the mapping block. Later the image was divided into non-overlapping sub-blocks with 8x8 sizes and sub-blocks classified into different types according to block variance. Experiments also shown that this scheme can detect and localize damage by 8x8 pixels and can recover 40% tampered image. The calculated tamper detection accuracy and values were recorded for blocks of some various sizes. **"The smaller the block size is, more accurate the tamper localization is"**

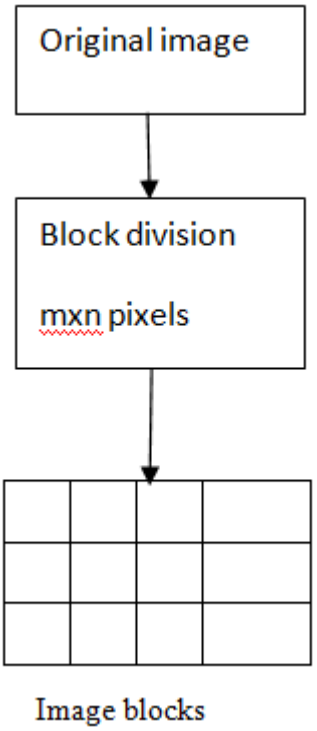


Fig. 7 Block wise division of image

Block Mapping Sequence:

In the self-embedding watermarking scheme, block mapping is done before the watermark insertion process. In this case, a certain block feature will be inserted as watermark payload for another block. The block mapping is generally grouped into linear transformations:

1. 2-D Transformations[5]
2. 1-D Transformations

In 2-D transformation can be expressed by an expression

$$A = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix}, \begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = A\, x \begin{pmatrix} x_i \\ y_i \end{pmatrix} \ mod\ N$$

Where a point (x_{i+1}, y_{i+1}) can be transformed from another point (x_i, y_i) and $(x_i, y_i) \in [0,N-1] \times [0,N-1]$ and $k \in [0,N-1]$, N is the total number of blocks in the image.

For 1-D transformation, a one-to-one mapping sequence was obtained as shown below

$$X' = [\, f(X) = (k * X) \bmod N] + 1$$

Where X, X [0,N-1], k is a secret key and N is the total number of blocks in the image .

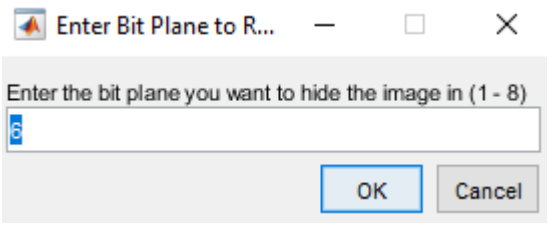
However, due to the limited number of degrees of freedom, linear transformations can be easily reconstructed by only experimenting with some images, and other weakness are low security. To solve this problem we have proposed a nonlinear block mapping construction using a pseudorandom sequence. A block mapping sequence B is computed from a key based pseudorandom permutations $[B(1)\ldots B(N)]$ of the integer interval $[1\ldots N]$. Where for an even number key, on 1-D transformation there is a repetition, so it does not produce one-to-one mapping.

3.3 Watermark Generation:

The watermark embedding phase occurs at the sender's side. As mentioned earlier, the first step is the original image divided into non overlapping blocks of size mxn. Then the block mapping method is used to generate a chaotic map (graph). Next step is generating authentication data and feature information as recovery data, both of them form watermark component. For watermark generation we need to generate two authentication bits:

The generation of first authentication bit was using the most significant bit (MSB) value. In this method we are using 5 MSB bits of 8 binary bits, while 3 bit LSB values for the insertion process are used.

1. 8 bit binary conversion of each pixel.
2. Set 3 LSBs of each pixel to zeros.
3. 8 bit binary conversion of row value of each pixel.
4. 8 bit conversion of column value to each pixel.
5. Bind pixel value with row value.
6. Bind pixel value with column value.
7. Generate a random number key_2 using a seed value.



$$key_1 = \text{mod}\ (key_2, 16)$$

8. Convert the decimal value into binary.
   $k_2 = \text{dec2bin}(key_2, 4)$
   $k_{4x1} = M \times k_2'$
   $a^1 = \sum_{m=1}^{4} (k(m)) mod\ 2$
9. Similar to a^1, a^2, a^3 and a^4 calculated for remaining 3 pixels of the block.

Authentication bit1,

$$A_{b1} = \sum_{m=1}^{4} (a^m) mod\ 2$$

Procedure for generation of First Authentication Bit:

This method used check bit as the part of bit authentication; it implemented a random redundancy check and pixel mean values of each block.

1. Delete the 3 LSBs from each pixel.
2. Mean value of nth block pixels.
3. Start the loop for thresholding

Thresholding:

Image thresholding is a simple, yet effective, way of partitioning an image into a foreground and background. This image analysis technique is a type of image segmentation that isolates objects by converting grayscale images into binary images. Image thresholding is most effective in images with high levels of contrast.

The simplest thresholding methods replace each pixel in an image with a black pixel if the image intensity is less than some fixed constant T or a white pixel if the image intensity is greater than that constant. In the example image on the right, this results in the dark tree becoming completely black, and the white snow becoming completely white.

4. Apply threshold m on each pixel and generate binary matrix m_b.
5. Convert into single bit a_1.
6. Organize a matrix M.
7. Apply LRC function
8. Again convert it into singe bit a_2.
9. Second authentication bit:

$$A_{b2} = a_1 \oplus a_2$$

3.4 Watermark Embedding

In spatial domains, two watermarks are generated from the sender's side, i.e., detection bits and recovery bits. On the decoder side for the authentication phase the watermark component is extracted to check whether there are any malicious modifications or not. If there is any tampered image, the watermark can be used to determine the tampered part. The important thing that needs to be underlined is the section of watermark components for recovery process. In addition the more watermarks are inserted, more the formation about verification and recovery can be maintained. Therefore, more watermarks generally result in more accurate tamper detection and improved recovery quality.

However the number of watermarks should be selected while still protecting the image from serious distortion. Therefore we must choose simultaneously between the accuracy of tamper detection and the quality of recovered image, while preserving the image quality that watermarks should be considered studies Self-embedding watermarking scheme helps to improve the quality of restored image. It compares the use of average intensity of blocks with the watermarking bits in varying length.

3.5. Tamper Detection and Recovery of Watermark

Tamper Detection:

After the watermarked image is sent, a receiver will detect if there is any modification caused by public channel using detection bits. For each block in the suspicious watermarked image, we segment the watermark extracted from the 3LSB[9] bit into two segments, i.e., recovery bits and detection bits vector with the same secret key on the transmitter. Then, it is compared with the detection bit vector. If the blocks get the same value, then the block is marked as authentic block.

Tamper Recovery:

After detection process, either the authentic or inauthentic bock can be identified. This method only restores an inauthentic bog, while authentic blocks are maintained the same. For the invalid blocks [8], its corresponding block is used to find recovery information**.**

If the part of watermarked image is damaged, the watermark data in that area can still be retrieved. If the amount of extracted data is greater, it will be able to reconstruct the original coefficient in the tampered area according to the given constraint. Smaller the damaged area, the available watermark data will result in better quality recovered content.

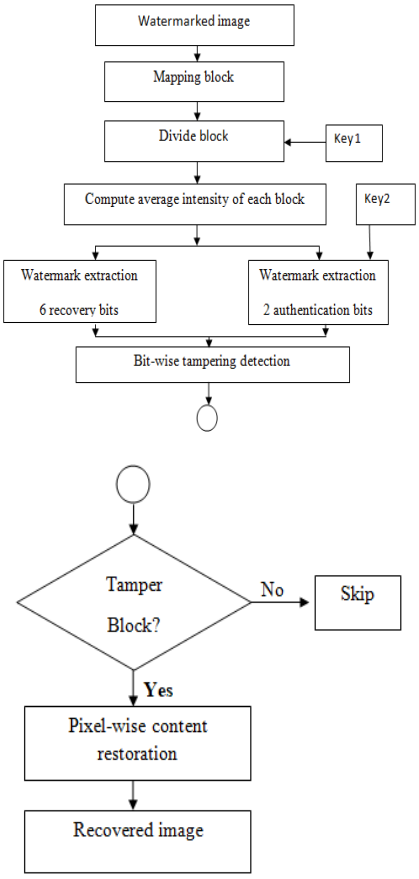


Fig. 8. Water mark recovery process

Fragile watermarking methods have been used with better restoration capabilities and can be applied in different types of images. It facilitates the ability to detect tamper hierarchically, where this process can locate areas damaged up to 3 levels. If it is not found in first level, it will continue to the second level and third level. In this scheme, it is not possible to recover the damaged block when the watermark that is inserted into another block is also damaged and there is no second chance to recover the block is shown in fig 8.

The problem for other opportunities for restoration of the block was assigned to solve the accidental problem of interference by installing two copies of restoration bits into the image. Increasing the watermarking capacity leads to a

quality decrease of watermarked image which uses 3 bits of the LSB to store bit recovery. To improve the quality of watermarked images and restoration of damaged images we use adaptive bit allocation mechanism. This method inserts a watermark into one LSB with the ability to change the length of the block image encoding results based on the smoothness of the block [3, 5]. On the side of the decoder, if the extraction of the decoder length is not suitable, it cannot show where the image is damaged; some additions of authentication bit components can degrade the image quality itself.

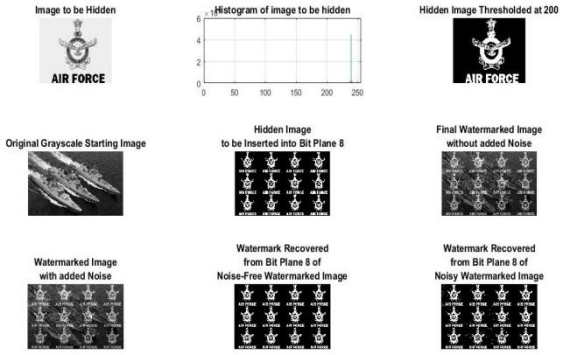


Fig. 9 Results of bit plane 1

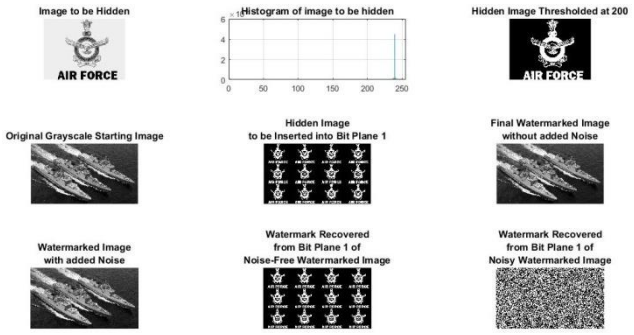


Fig. 10 Results of bit plane 2

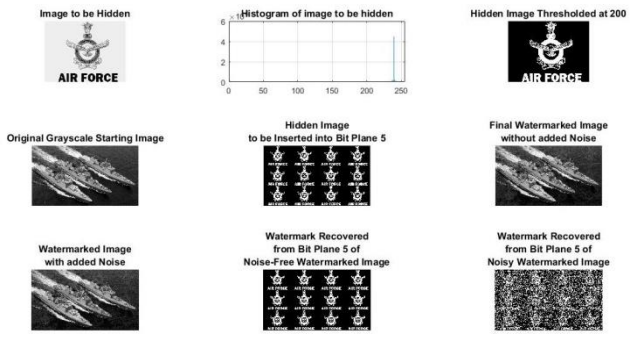


Fig. 11 Results of bit plane 5

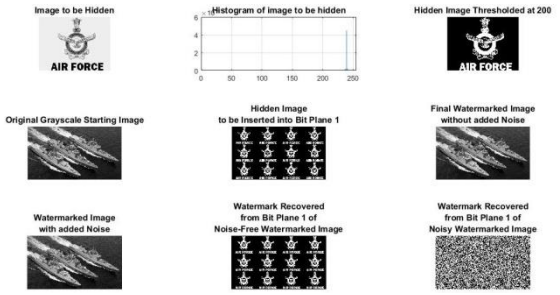


Fig. 12 Results of bit plane 7

Conclusions:

There are two water watermarks which are used for authentication with recovery capability: authentication bits and recovery bits. Authentication bit is for tamper detection and localization, while restoration bit is for tamper recovery in decoder side. In spatial domain, the watermark is selected from the image figure itself which is then inserted in LSB bit-plane by first emptying the bits at the position one LSB, two LSB and three LSB, where the bits will be used for detection in case of damaged and it can be extracted to replace the tampered bit. Therefore the watermark image quality depends entirely on the amount of LSB replaced by watermark pixels.

As discussed in the paper, if the invisibility of the watermark is high then, then the data will be hidden and an unauthorized person couldn't get it because of insertion of noise added by him and the data gets damaged. It can only be recovered if we know the authentication and recovery keys.

As our motive is military data authentication so high level security is required, so this fragile watermarking technique plays a crucial role in the image authentication and it will not allow the unauthorized user to recover even a bit of information.

References

1. D.Singh, S.K.Singh, Effective self-embedding watermarking scheme for tampered detection and localization with recovery capability. J.Vis. Commun.Image Represent.38,775-789(2016).https://doi.org/10.1016/).jvcir.2016.04.023

2. C. Qin, C. Chang,P. Chen, Self-embedding fragile watermarking with restoration capability based on adaptive bit allocation mechanism.Signal process.92, 1137-1150(2012).https://doi.org/10.1016/j.sigpro.2011.11.013
3. J. Chang, B. Chen, C Tsai,"LBP-based fragile watermarking scheme for image tamper detection and recovery," 2013 International Symposium on Next-Generation Electronics (Kaohsiung, 2013),pp. 173-176.https://doi.org/10.1109/ISNE.2013.6512330
4. R. Chamlawi, I. Usman, A. Khan, "Dual watermarking method for secure image authentication and recovery," 2009 IEEE 13th International Multitopic Conference (Islamabad, 2009), pp. 1-4. https://doi.org/10.1109//INMIC.2009.5383118
5. A recent survey of self-embedding fragile watermarking scheme for image authentication with recovery capability,Lusia Rakhmawati, Wirawan Wirawan ,*EURASIP Journal on Image and Video Processing* volume 2019, Article number: 61 (2019)
6. S. kiatpapan, T.kondo, in 2015 12th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON). An image tamper detection and recovery method based on self-embedding dual watermarking (Hin, 2015), pp,1-6. https://doi.org/10.1109/ECTIC.on.2015.7206973
7. X.Zhang, S. Wang, Z. Qian, G. Feng, Reference sharing mechanism for watermark selfembedding. IEEE Trans. Image Process.20(2), 485-495(2011).

   https://doi.org/10.1109/TIP.2010.2066981
8. F. Cao, B. An, J. Wang, D.Ye, H. Wang, Hierarchical recovery for tampered images based on watermark self-embedding correspondence. Displays , 46.52-60(2017), https://doi.org/10.1016/j.displa.2017.01.001
9. C. K. R, N. Shivananda, in 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI). A new fragile watermarking approach for tamper detection and recovery of document images (New Delhi, 2014), pp. 1494–1498. https://doi.org/10.1109/ICACCI.2014.6968624