ISSN 2394-3777 (Print)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 14, March 2016

ROBUST WATERMARKING TECHNIQUE USING FQTS AND HISTOGRAM SHIFTING

Arthy.R[1] , Bavithra.K[2], Suvitha.J[3] ,Karthiga.K[4]
[1, 2,3,4] Department of Information Technology
Kamaraj College of Engineering and Technology
arthyit@kamarajengg.edu.in

ABSTRACT

A Robust watermarking is a technique to retrieve the secret image (gray image) without any distortion from the watermarked image. A series of reversible watermarking techniques have been proposed to increase embedding capacity and the quality of the watermarked image simultaneously. In this paper reversible watermarking is proposed using fuzzy matching quad tree segmentation technique. Quad tree is a hierarchical representation in which a node represents blocks of white, black or gray pixels. Histogram shifting is applied for embedding encrypted watermark image into cover image to obtain watermarked image. The watermarked image is tested against various attack to ensure that the proposed reversible watermarking algorithm withstands the attacks. The performance of the proposed method is measured by calculating PSNR value and MSE value. The Quad Tree segmentation ensure high performance by yielding high PSNR value. Thus, the proposed algorithm is robust against various attack and provides high performance. It also preserves the image quality.

Keywords: Watermarking, Histogram Shifting, Fuzzy Matching, Quad Tree.

I.INTRODUCTION

Digital watermarking is the act of hiding a message related to a digital signal (i.e. image, audio, video) within the signal itself. It is used to identify the ownership of copyright information about image. Digital watermarks cannot be removed or altered. It allow users to legally use content, while adding security to the image to prevent illegal usage against hackers. Digital watermarks are "robust," means that they are not able to perform attacks from potential hackers , in addition they provide information about the original image.

A.WATERMARKING TECHNIQUE

Digital watermarking involves two major operations. They are (i) watermark embedding, and (ii) watermark extraction. For both operations a secret key is needed to secure the watermarked image. The important properties of digital watermarking techniques are: robustness, security, imperceptibility, complexity, and verification. Watermarking techniques can be classified according to the nature of data (ie text, image, audio or video), or according to the working domain (spatial or frequency).In images, the watermarking techniques can broadly be classified into two types: (i) visible watermark, (ii) invisible watermark.

B.WATERMARKING DOMAINS

Watermarking are usually embedded in spatial or frequency domain. Spatial domain embedding is a linear operation that directly deals with the host image bytes one by one consequently. Frequency domain embedding is a nonlinear operation that deals with the frequency components of the host image. In this paper spatial domain concepts are used for watermarking.

C. QUAD-TREE SEGMENATION

A quad-tree is a data structure that refers to a hierarchical representation of blocks that are partitioned into four blocks. Payload can be calculated for the cover image, and then it will partition into four blocks of same size. And then calculate the individual payload for the four blocks. If the total payload is greater than individual payload again the block is divide into four blocks. These steps are repeated to obtain the secret key(bit stream). Else partition is not needed for the cover image.

ISSN 2394-3777 (Print)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 14, March 2016

II. LITERATURE SURVEY

Neethu V. Gopal and Madhu S [1] proposed Fuzzy Art Based Geometrically Invariant Robust Watermarking Scheme. This method fuzzy art clustering and image normalization that is to overcome the attack. Fuzzy art is for accurate selection of location and also for invisblity.

Huawei Tian, Yao Zhao and Rongrong Ni [2] presents the watermark scheme for robust against desynchronization attacks. In this paper BSP tree is used for partition. It is fixed under global transform and local transform and cropping.BSP tree uses logarithmic quantization index modulation for watermarking embedding method. The drawback is that the detector fails to extract the watermark.

G.Roseline Nesakumari, L.Sumalatha and V.Vijayakumar [3] projected the Fuzzy Based Chaotic and Logistic Method for Digital Watermarking Systems to provide the authentication, security and robustness. This paper make use of FCL method to modify the original image into transform domain, and Logistic map is used to determine the bit position of host image. These techniques are used to overcome the pseudo random property, self reference scheme and sensitive dependence.

Priyanka D. Godsae,Snehal B.Kale, Sonika S. Shelke, S.M.Sangve and S.P.Deshmukh [4] proposed the Robust digital watermarking for colour images using Fuzzy vault. The important issue arises in the paper is the protection of the rights for all participants. The DCT algorithm was applied to the copy right protection of the image by inserting fuzzy vault into the host image It make use of DCT method for watermarking to withstand a variety of image processing.

In[5], Hung-Hsu TSAI and Shih-Che LO achieved the deadlocks and failed to get track of clues regarding piracy. The watermarking scheme uses the JND profile and Fuzzy Inference System optimized with genetic algorithm called AIWFG. FIS generated with the image features and local statistics of the watermarked image. But it is failed to met the blurring and stirmark attacks.

Yih-Chaun Lin and Tzung-Shian Li [6] presented the Reveresible Image Data Hiding Using Quad-tree Segmentation and histogram shifting. They used the input message and it can be split into several sized block of pixels and they are organized into tree structure. The main advantage of using this approach for quality of image, not for a specific type of image and execution time is less.

In [7] Y-T Wu and F.Y.Shih proposed the steganalytic techniques to detect whether an image contains a hidden message. By analyzing various image features between stego-images (the images containing hidden messages) and cover-images (the images containing no hidden messages), a steganalytic system is able to detect stego-images. It is to increase the capacity of the embedded message and enhance the peak signal-to-noise ratio of stego-images.

III.PROPOSED METHODOLOGY

Cover Image

RGB image is used as cover image in the proposed method. This cover image contains no hidden message. It is segmented using Fuzzy based Quad - Tree Segmentation.

Quad-Tree Segmentation

A quad -tree is a tree data structure in which each internal node has exactly four blocks. These blocks are formed by splitting the cover image and organized as a form of quad -tree structure. In the quad-tree segmentation process, the first step is to make a decision on whether a further division is required or not. After this, calculate the payload for whole image. Then the payload is found out for each sub blocks individually. If the total payload size of the four block is larger than that of incoming block, then the incoming block is divided into another four sub blocks. This process is continued until each blocks size reaches 32 Pixels. Formula for calculating the payload:

payload=max1-log2(m)*min1-16;

Algorithm:

Input:RGB cover image
Output:Bit-Stream
Begin
step 1: split into 4 blocks and find the size of the cover image as matrix
Step2:Apply histogram for cover image then sort the pixel values
Step 3:Assign maximum and minimum point and calculate total payload for whole image(ps1)

ISSN 2394-3777 (Print)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 14, March 2016

Step 4: Repeat step 3 for each quadrant
Step5: Add each quadrant payload(ps3)
Step 6: if ps3>= ps1
num=1
qtde(r(1:m/2,1:n/2),srt(1:m1/2,1:n1/2));
qtde(r(1:m/2,1:n/2+1:n),srt(1:m1/2,1:n1/2+1:n1));
qtde(r(1:m/2+1:m,1:n/2),srt(1:m1/2+1:m1,1:n1/2));
qtde(r(1:m/2+1:m,1:n/2+1:n),srt(1:m1/2+1:m,1:n1/2+1:n1));
step 7:elseif ps3<ps1
num=0
end
end

Where m and n are the rows and columns of cover image, r is the cover image, m1 and n1 are the rows and columns of the secret image and srt is the secret image.

Secret Image

Gray image is used as a secret or logo image. This gray image is converted into binary image. Performing the XOR function, we encrypt the secret key and binary image. After this we get the encrypted logo image.

Histogram shifting

A histogram is a statistical information that uses rectangles to show the frequency of data items in successive numerical intervals of equal size.

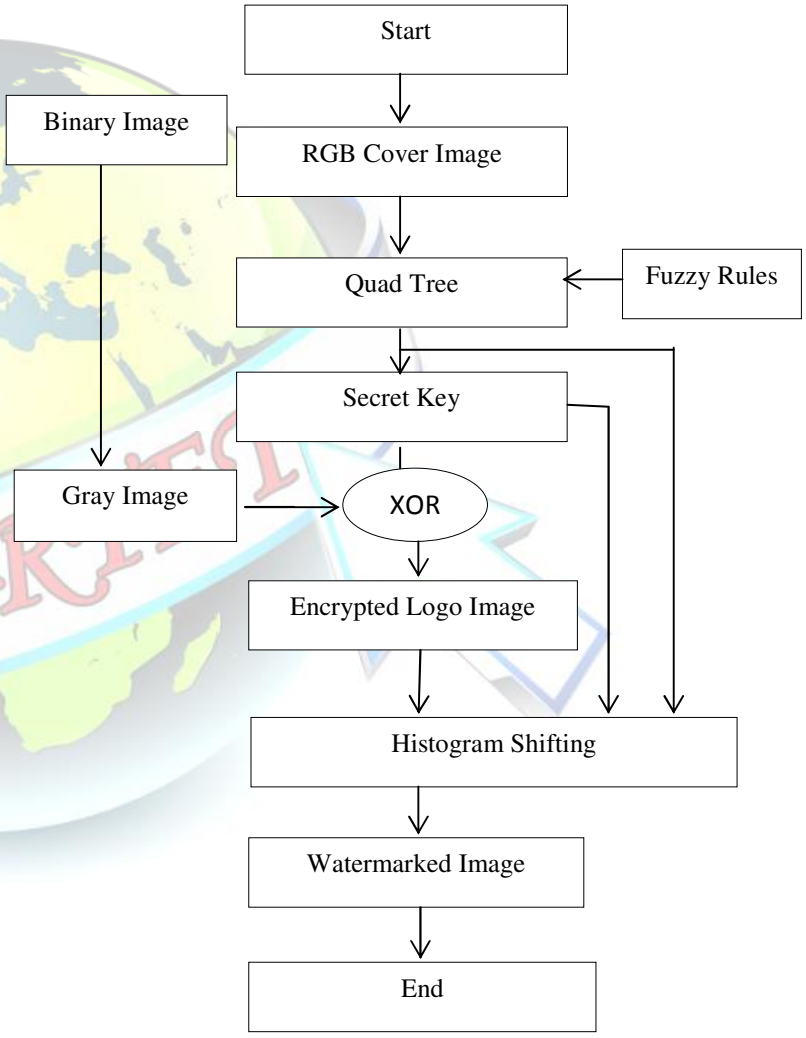
Fuzzy Rule

If sum of all blocks of the incoming payload is greater than or equal to total payload, then the incoming block is again partitioned into four sub blocks and binary variable is set to one.

$$ps3=ps11+ps12+ps13+ps14$$

Embedding Process

In embedding process, RGB image is taken as a cover image and gray image as a secret image which it is converted into binary image. RGB image is partitioned using quad tree segmentation by calculating the payload. This generates the secret key. Using XOR function, we encrypt the binary image and the secret key. By this, we obtained the encrypted logo image. The quad tree blocks and encrypted logo image is embedded using Histogram shifting. Finally the watermarked image is obtained.

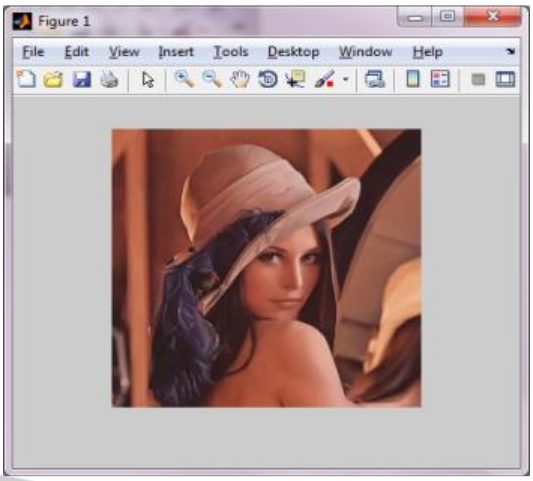


Extraction Process

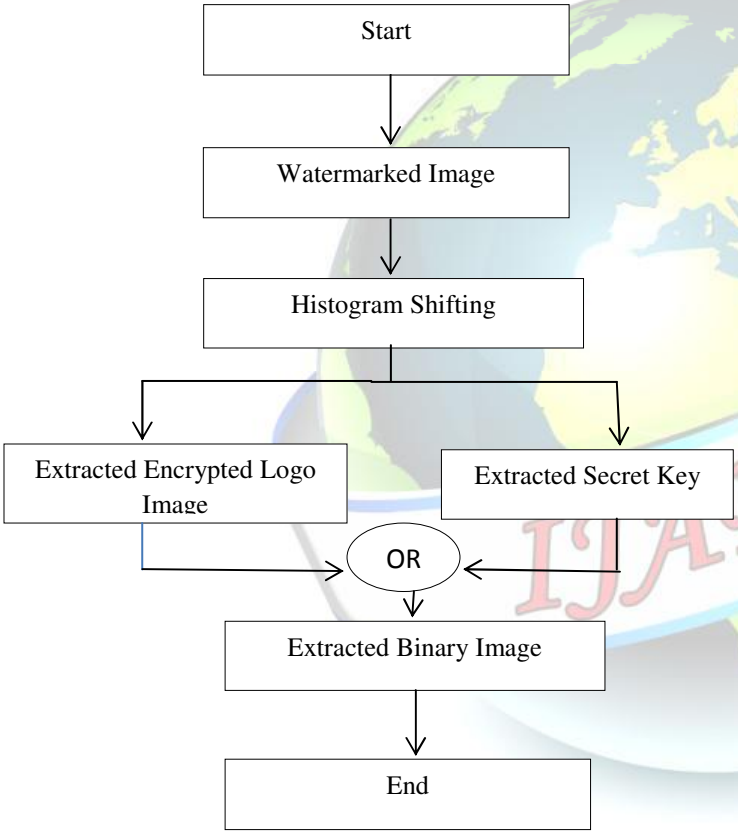
After performing the attacks, extraction process is done. In extraction we use the reverse

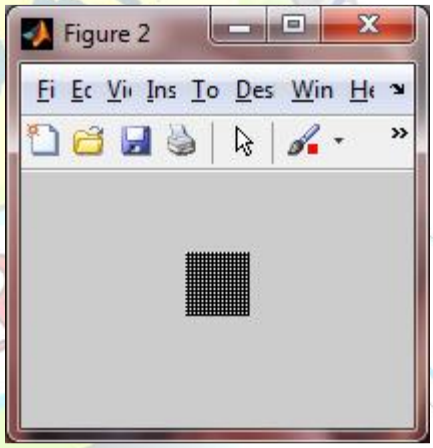
ISSN 2394-3777 (Print)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 14, March 2016

histogram shifting. This extracts the encrypted logo image and the secret key. After this, we perform the XOR function with these encrypted logo image and the secret key. Finally we obtain the secret image.

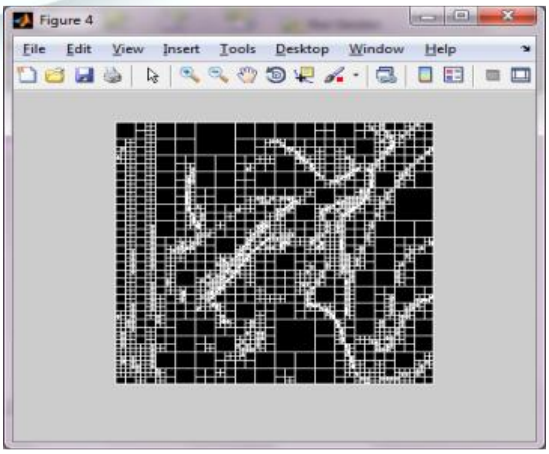


Secret image





Quad tree segmented image



IV. RESULT AND DISCUSSION

RGB is used as a cover image which contains no hidden message.Binary image is used as secret image.

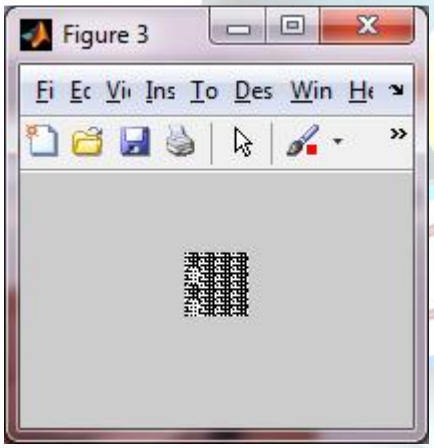
RGB Cover Image

ISSN 2394-3777 (Print)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 14, March 2016

Total Payload=1322

Quadrants	Payload
First quadrant	347
Second quadrant	408
Third quadrant	615
Fourth quadrant	337

Encrypted image



V. CONCLUSION

In this paper both extraction and embedding was done with the help of applying fuzzy based quad tree segmentation to generate the secret key. And the histogram shifting is applied for the secret key, encrypted logo image and quad tree segmentation to obtain the watermarked image. In Extraction, reverse process is performed to obtain the secret image.

VI. REFERENCES

[1] Neethu v.Gopal and Madhu s. Nair"Fuzzy Art Based Geometrically Invariant Robust Watermarking Scheme"Engineering Letters,vol.22,2014

[2] Huawei Tian, Yao Zhao and Rongrong Ni,"LDFT-Based watermarking resilent to local desynchronization Attacks",IEEE Transactions on cybernetics,vol 43,pp.2190-2201,2013

[3] G.RoslineNesakumari, L.Sumalatha and V.Vijayakumar, "Fuzzy Based Chaotic and Logistic Method for Digital Watermarking Systems", International Journal of Scientific & Engineering Research Vol. 3, 2012

[4] Priyanka D. Godase, Snehal B. Kale, Sonika S. Shelke, S.M.Sangve and S.P.Deshmukh, "Robust Digital Watermarking for Color Images Using Fuzzy Vault", Global Journal of Computer Science and Technology, Vol. 12, 2012

[5] Hung-Hsu TSAI and Shih-Che LO, "JND-Based Watermark Embedding and GA-Based Watermark Extraction with Fuzzy Inference System for Image Verification", Informatica, Vol. 25, 2014

[6] Yih-Chuan Lin and Tzung-Shian Li, "Reversible Image Data Hiding Using Quad-tree Segmentation and Histogram Shifting", Journal of Multimedia, Vol. 6, pp.349-358, 2011

[7] Y.-T.Wu and F. Y.Shih, "Genetic algorithm based methodology for breaking the steganalytic systems," IEEE Trans. Syst., Man, Cybern. B, Cybern, Vol. 36, no. 1, pp. 24–31, Feb. 2006.