ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

A Novel Digital Blind Watermark Embedding Process Using Gain Control Tamper Detection Algorithm

M.Mangaiyarkarasi[1], Dr.R.Gunavathi[2]

Research Scholar, Sree Saraswathi Thyagaraja College, Pollachi, Tamilnadu, India[1]

Head of Department, Dept. of Computer Applications, Sree Saraswathi Thyagaraja College, Pollachi, Tamilnadu, India[2]

ABSTRACT: Watermarking techniques is the application of digital image processing domain to discover patterns from the real-world images. In Digital watermarking, image or video is embedded information data within an insensible form for human visual system but in a way that protects from attacks such as common image processing techniques. This research presents a framework for digital image watermarking with steganography process to discovering best feature from Noisy image database. By aligning the important image features from the database and by using the matching sequence or its encryption of match, the searching between the data features are determined. The proposed research work presents a new approach to measure the blind features in image database using the methodologies Image feature extraction is characterized by a pre-processing analysis where the color feature values are transformed into luminance value. The blind watermark embedding method gives a useful measure is used to hide a cover object locations in terms of their image features property. Some of the challenges faced in finding the lossless and exact authentication of relational databases via expansion on data error histogram. This research proposes an enhanced Blind Gain control tamper detection (BFCT) algorithm to estimate the watermarking process using minimal redundancy optimization method corresponding database.

KEYWORDS: Image Feature Extraction, Watermark embedding, Blind embedding and linear correlation detection and Gain control tamper detection extraction.

I. INTRODUCTION

Digital watermarks are employed in an attempt to provide proof of ownership and identify illicit copying and distribution of multimedia information. Digital watermarking describes methods and technologies that allow hiding information, for example a perceptually invisible pattern (watermark) can be embedded into the image and ideally would stay in the image as long as the image is recognizable (Figure 1). Another purpose of digital watermarks is to enable detection of image tampering. The hiding process has to be such that the modifications of the pixel values have to be invisible. Furthermore, the watermark has to be robust or fragile to resist to manipulations of the media, such as lossy compression, scaling, and cropping, just to enumerate some.

Image authentication and tamper detection techniques based on Digital Watermarking technology exist and are being used by many imaging companies, but the major drawback of this approach is that the code to be embedded must be inserted during the capture and recording of the digital image. This can be only possible with specialized cameras i.e. cameras need to be adapted for Digital Watermarking. This method though mentioned as imperceptible and robust, is only an assumption, and there is no guarantee that the embedded code cannot be read and rewritten in to the image after tampering or robust to all kinds of basic image processing operations and compression techniques.

Image tampering is defined as “adding or removing important features from an image without leaving any obvious traces of tampering”. In terms of image processing, tampering can be defined as changing original image information by modifying pixel values to new preferred values so that the changes are not perceivable. This means enhancing an image by tampering the image in order to clearly express the information content of the image should not be taken as tampering, but tampering to deliberately doctor digital images from their time of capture with an intention to change its original information is called digital image tampering. It is also called as image forgery.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

II. RESEARCH METHODOLOGY

The proposed architecture accepts the digital image parameters as input which contains the MATLAB simulation where the optimal image watermarking and stenography algorithm is applied to the real-world image databases.

A. THE PROPOSED SYSTEM

Digital images are easy to control and alter due to accessibility of dominant image processing applications and editing software. The need for validating digital images is to replace analog counterparts with digital and video cameras, will increase detecting forgeries and the content is validated. In particular, the proposed system focus only on detection of a particular type of digital forgery – the Gain control algorithm in which a piece of an image is copied and pasted somewhere in the image with the purpose to cover an important imaging feature.

B. IMAGE FEATURE EXTRACTION

A color image is a combination of some basic colors. In each individual pixel of a color image (termed 'true color') classified into Red, Green and Blue values. The extracted features of RGB color should never be changed to different geometric and photometric changes and should have minimal data to discriminate between the object which they define and other objects. The digital images convey information at different levels and in order to represent most of the image information, it is necessary to use different features at the same time. Therefore, the work proposed, extracts many features from images to represent the color and texture. The most widely used image descriptors is color histogram and it represents the color distribution of an image. It possess several valuable properties such as robustness, compactness, and invariance with respect to the geometric transformation of the original image like scaling and rotation.

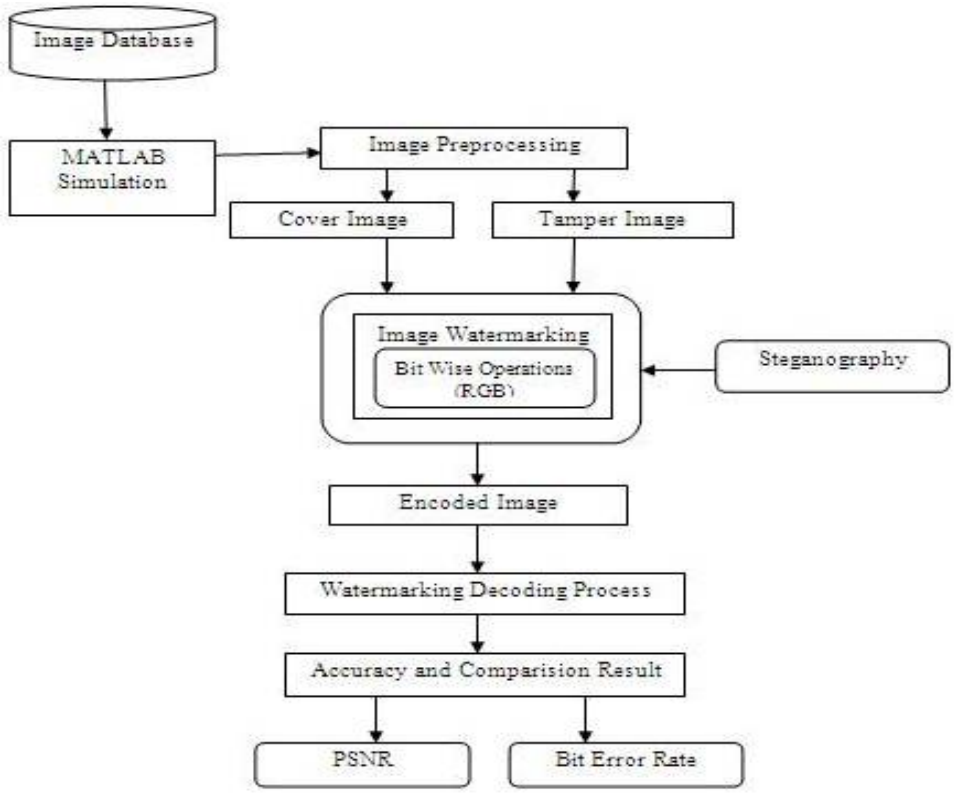

Fig. 1. Architecture of Proposed System

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

C. WATERMARK EMBEDDING

The watermark should be unnoticeable so as not to affect the screening experience of the image or the quality of the audio signal. The watermarking algorithm should embed the watermark in some watermarking applications, it does not affect any quality of data. A watermark embedding practice is truly invisible, if humans cannot differentiate the original data with inserted watermarked content. Though less modification in the data may become obvious when the original data is evaluated directly with the watermarked information. As users of watermarked content normally do not have access over the original information, they cannot perform any comparison. So it may be adequate, that modification in watermarked content is unobserved as long as the data are not balanced with the original content. The exact level of robustness the hidden data must possess cannot be specified without considering a particular application.

Let the image be denoted by I and the series of covariance's be $Covr = c_1, c_2 \ldots, c_n$ were n is length of watermark image. The series of covariance's $Covr$ are the largest (most significant) in the DCT domain.

The watermark Embedding can be altering the covariance's by the following formula:

$$Covrr\_I' = Covrr\_I + a\ X\_I \quad \text{eq. (1)}$$

D. BLIND EMBEDDING AND LINEAR CORRELATION DETECTION

This system is an example of blind embedding, which does not exploit the original image statistics to embed a message in an image. The detection is done using linear correlation. This system is a 1-bit watermarking system, in other words it only embeds one bit (a 1 or 0) inside the cover image.

Detector

- Compute the linear correlation between the watermarked image that was received and the initial reference pattern that can be recreated using the initial seed which acted as the watermarking key.

Decide what the watermark message was, according to the result of the correlation. If the linear correlation value was above a threshold, we say that the message was a 1. If the linear correlation was below the negative of the threshold we say that the message was a 0. If the linear correlation was between the negative and the positive threshold we say that no message was embedded.

E. GAIN CONTROL TAMPER DETECTION EXTRACTION

Image tampering normally distorts image statistics inside tampered image section. So, it is probable that tampered image regions must yield different de-mosaicing artifacts as compared to the rest of the image portion. Due to safety measures, the watermark pattern should depend on the block. To extract M bits from each block and make a spread spectrum noise-like signal from this M-tuple. Since it need to be extract the watermark from distorted images, to call for a process that would present us the same M-tuple for all similar looking blocks. A Gain control tamper detection (GCT) algorithm is an step by step procedure for finding maximum likelihood method in statistical models, where the model depends on finding the unobserved secret key variables.

III. PSEUDO CODE

Step 1: Load the input image and tamper watermark image.
Step 2: Calculate the geometric models for watermark embedding using eq. (1).
Step 3: Insert the encryption key range (0-255) during the blind embedding linear correlation detection.
Step 4: Calculate the image feature watermark embedding process.

```
if (encryption key = =matched)
        Make the extraction process.
else
      break;
end
```

Step 5: The key is calculated using GCT algorithm.
Step 6: The output image is extracted with the secret key.
Step 7: End.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

IV. PERFORMANCE EVALUATION

The research work and the experiments are performed to evaluate the imperceptibility of the embedded watermark as well as the robustness of the proposed watermarking scheme against various attacks. In our experiments, we use two set of gray scale images of size 512 x 512, obtained from [23] and [24]. Table I & II gives the peak signal-to-noise-ratio (PSNR) and bit error rate (BER) values obtained using the proposed watermarking scheme with two different contourlet filters for some of the test images. It is seen from this Table that the 9-7 biorthogonal filter is a better choice in our watermarking scheme, since it provides higher PSNR values for the watermarked images along with lower BER when the watermarked images are contaminated by Gaussian noise. Therefore, we obtain the rest of the results using 9 - 7 biorthogonal filters. The original and watermarked images for two of the test images, namely, Barbara and Lena, as well as the absolute difference between the watermarked and the original image.

A. *COMPARISON OF PSNR VALUES*

Peak Signal-to-Noise Ratio (PSNR), defines the ratio between the maximum possible power of a signal and the power of humiliating noise which affects the reliability of its representation. Since wide dynamic range differ based on signals, PSNR is generally measured in terms of the logarithmic decibel scale (dB).

The PSNR fraction measure is quality of reconstruction. PSNR is an approximation to human perception of reconstruction quality. Higher PSNR generally indicates that the reconstruction is of higher quality.

The Peak signal noise ratio is calculated for all five images using the formula,

$$PSNR = 20 * \frac{log_{10}(MAX_I)}{std(ERROR)} \quad (2)$$

Images	Pkva	9-7	Proposed
Barbara	52.10	52.38	53.25
Lena	55.13	55.58	56.47
Baboon	50.94	51.47	52.28
Boat	53.73	54.38	55.92

Table 1. PSNR Measures for the Three Methods

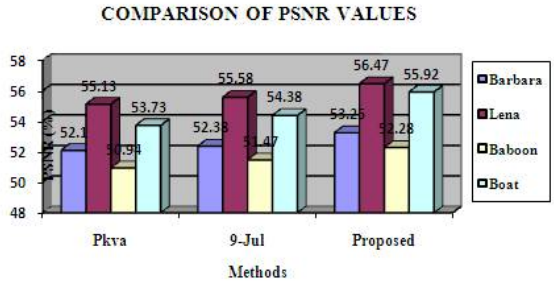

Fig. 1. Comparison of PSNR Measures

B. *COMPARISON OF BIT ERROR RATE VALUES*

A bit error rate is defined as the rate at which errors occur in a transmission system. This can be directly translated into the number of errors that occur in a string of a stated number of bits.

The definition of bit error rate can be translated into a simple formula:

$$BER = \frac{Number\ of\ errors}{Total\ number\ of\ bits} \quad (3)$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Images	Pkva	9-7	Proposed
Barbara	11.5	7.9	7.2
Lena	9.8	6.1	5.7
Baboon	10.4	7.8	6.82
Boat	8.4	5.9	4.58

Table 2. BER Measures for the Three Methods

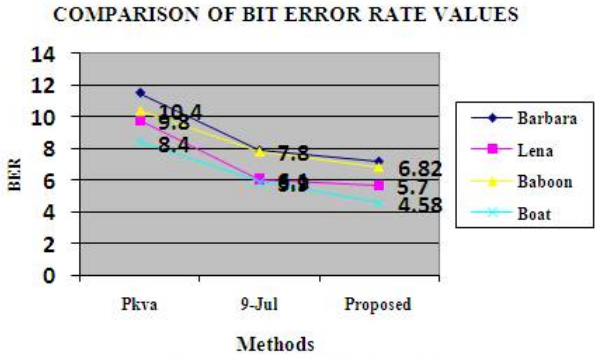

Fig. 2. Comparison of BER Measures

V. CONCLUSION

This research presents an enhanced method such as Digital image watermarking based on Blind Gain control tamper detection (BFCT) algorithm which combines watermarking and Stenography methods to solve the problem of forgery detection applications. In the BFCT model, some of the new training features will be selected using the knowledge currently held by the system. Then, specific features will be extracted from selected training image features. The proposed methodologies performance is analyzed with real-world image databases those are downloaded from image database repository. The values are compared with several constrains such as number of dimensions versus objective, PSNR and BER. Based on the results generated this research concludes that accuracy increases compared to the previous method of Contourlet Domain algorithm.

REFERENCES

[1] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, 1997.
[2] C. J. Cheng, W. J. Hwang, H. Y. Zeng and Y. C. Lin, "A fragile watermarking algorithm for hologram authentication," Journal of display technology, vol. 10, no. 4, pp. 263-271, 2014.
[3] G. Coatrieux, W. Pan, N. C. Boulahia, F. Cuppens and C. Roux, "Reversible watermarking based on invariant image classification and dynamic histogram shifting," IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 111-120, 2014.
[4] H. Sadreazami, M. O. Ahmad and M. N. S. Swamy, "A study of multiplicative watermark detection in the contourlet domain using alphastable distributions," IEEE Transactions on Image Processing, vol. 23, no. 10, pp. 4348-4360, 2014.
[5] M. M. Rahman, M. O. Ahmad, and M. N. S. Swamy, "A new statistical detector for DWT-based additive image watermarking using the Gauss-Hermite Expansion," IEEE Transactions on Image Processing, vol. 18, no. 8, pp. 1782-1796, 2009.
[6] J. R. Hernndez, M. Amado, and F. P. Gonzlez, "DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure," IEEE Trans. on Image Process., vol. 9, no. 1, pp. 55-68, 2000.
[7] M.Mangaiyarkarasi, Dr.R.Gunavathi, "A Survey on Multiplicative Watermark Decoder in Contourlet Domain," International Journal of Modern Computer Science & Applications, vol. 4, no. 3, pp. 2321-2632 , 2016.
[8] M.Mangaiyarkarasi, "Digital Image Watermarking from Past to Future: An Overview," International Journal of Modern Computer Science, vol. 4, no. 4, pp. 2320-7868 , 2016.
[9] H. Sadreazami, and A. Amini, "A robust spread spectrum based image watermarking in ridgelet domain," International Journal of Electronics and Communications, vol. 66, no. 5, pp. 364-371, 2012.
[10] M. Zareian and H. Tohidypour, "Robust quantization index modulation based approach for image watermarking," IET Image Processing, vol. 7, no. 5, pp. 432-441, 2013.
[11] [Online]. Available: http://decsai.ugr.es/cvg/dbimagenes/index.php.
[12] [Online]. Available: http://bows2.ec-lille.fr/