ASIAN JOURNAL OF PHARMACEUTICAL AND CLINICAL RESEARCH

INNOVARE ACADEMIC SCIENCES
Knowledge to Innovation

Special Issue (April)

Online - 2455-3891
Print - 0974-2441
Full Proceeding Paper

A NOVEL IMAGE THEFT IDENTIFICATION USING BIOMETRIC FEATURE

JINCY J FERNANDEZ[1]*, NITHYANANDAM PANDIAN[1], RAGHUVAMSH CHAVALI[2], ASHWANTH KUMAR APPALAGHE[3]

[1]School of Computing Science and Engineering, VIT University, Chennai, Tamil Nadu, India, [2]Founder, Rashonic Unicpixel Technology Pvt. Ltd, Hyderabad, Telengana, India, [3]Co-founder, Rashonic Unicpixel Technology Pvt. Ltd, Hyderabad, Telengana, India.
Email: jincyj.fernandez2015@vit.ac.in

Received: 19 January 2017, Revised and Accepted: 20 February 2017

ABSTRACT

In today's internet world, all the data are represented and stored in digital form. Almost any entity in this world can be represented digitally, ranging from simple text to complex multimedia work. Now, the challenge is to claim the ownership and prevent theft of one's own digital data. Multimedia theft has driven the attention of many stakeholders who spend huge money and precious time in creating or making such valuable digital data. Among all the multimedia entities, image files are more vulnerable for theft since it is the basic component of any visuals. The notion of this research work is to propose an image theft detection model which will determine whether partial theft or complete theft of an image has occurred or not. A biometric feature, i.e., fingerprint of the owner is embedded on the digital image at a micro level, such that even a very small portion of image theft can be determined, and the ownership of the image can be claimed by the owner. This research is limited to the spatial domain, i.e. raw image. Assessment metrics of the results shows that embedding the biometric feature on an image does not distort the image quality and its artifacts.

Keywords: Digital watermarking, Content authentication, Ownership, Copyright protection, Fingerprint recognition.

 DOI: http://dx.doi.org/10.22159/ajpcr.2017.v10s1.19762

INTRODUCTION

Voluminous amount of multimedia contents is carried out by internet. The emerging need of social network and the deployment of many web servers lead to a massive increase of digital data eventually. Protecting such data against theft or illegal usage is a very big challenge [1], ahead of us. Among the various digital entities in cyberspace, digital image is a predominant medium, where each and every visual in this world is represented by image. Such image undergoes and satisfies many needs in the digital world ranging from simply viewing an image to authenticate a user by image. The images are created by the owner with tremendous effort and cost. Practically, we can realize it when we see great photographs placed in exhibits and recognized by prizes and awards. Hence, in this cyber world, it is imperative to claim the ownership of digital image [2] which we had created. Now, the question arises to us is that how to uniquely identify our digital work in this cyber world. Nowadays, digital acquisition medium can give you the date and time the picture was taken, even the geographical location where the picture was taken, but still claiming the ownership, i.e., who had taken the photograph remains an unsolved gray area problem. Binding the biometric property of our own unique physical feature [3] with the digital work we had created, is an elegant solution in proving the ownership of the digital work. The biometric characteristics of owner identity can be taken from any one of the following entities: Fingerprint, iris scan, retinal scan, etc. However, the most appropriate one for offering dynamic identity to the digital entity we had created using a camera in a mobile phone or a handycamera or a digital camera is our fingerprint.

Geographical attributes about an image [4] give information about "where the photograph was taken," similarly date and time specifies "when the photograph was taken." However, these data fail to give who had taken the photograph. It may be possible in real time that the camera owner may not be the real owner of the picture which was taken. Hence, to cater this special need, biometric trait of owner (who had taken the picture) should be bounded with the image that he/she had acquired through digital acquisition medium. It is an imperative state in the modern world, where digital theft has matured well in this society, and it should be prevented. Watermarking and fingerprinting are two different approaches to prevent the piracy of digital data [5]. Fingerprinting approach extracts a fingerprint from the image for verification [6]. Watermarking is a digital content authentication technique [7], where fragile or robust watermark [8] is embedded on the digital entity, namely, image, video, audio file, etc. The main functions of a watermark are the identification of the correct owner and tampering detection [9]. However, watermarking process does not put the metadata of the cover image on each and every pixel of the digital cover (with respect to image). It is highly complex to embed metadata on the entire digital cover. This limitation gives room for person who steals fragment of image pieces for their purpose and its goes unnoticed. It is possible to cut a fragment from multiple images or removing the vital segment of the image. To curb this activity, theft of each and every pixel of digital cover should be covered under vigilance. Stealing a very small fragment/segment should be determined.

The rest of the paper is organized as follows. Section II discusses the related works. The general matrix embedding technique is described in Section III. The proposed work is described in Section IV. Experimental results are given in Section V. The limitations of the proposed work are discussed in Section VI. Section VII gives the concluding remarks and future work.

RELATED WORKS

The increasing use of the internet has created a need for the security of multimedia data. Information protection is a critical issue to prevent the information which belongs to the respective owners from unauthorized access and usage. A very familiar and suggested technique is to insert watermark into multimedia data so that ownership can be proved. An efficient authentication scheme [10] should fulfill the following features:

1. Able to identify whether an image has undergone any modification or not
2. Able to identify the location of modification made on the image
3. Capable of integrating metadata to be authenticated within the cover image rather than as a separate data file
4. The embedded authentication data should be imperceptible.

Friedman [11] proposed an image authentication system, in which a digital signature is produced using camera's unique private key and the captured image. The digital signature is inserted at the time of storing

the image using a digital camera. In the verification phase, the image in question, its digital signature, and the public key unique to the camera are considered. The hash code of the image in question and the hash code of the original image are extracted and compared. If a match occurs, it indicates that both images are identical. Hsieh *et al*. [5] used fingerprint image as watermark. First, the fingerprint image is enhanced, and then a two-level Haar wavelet is applied on the cover image to generate features from the transformed coefficients in the LL2 subband. Moreover, a set of share images is generated to protect the image copyright. Voice signal of the content owner is considered as watermark by Saxena *et al*. [12]. The analog voice signal is digitized and represented in binary form, which in turn get embedded into the cover image. Rao *et al*. [13] used the technique of embedding singular values obtained from the shuffled coordinates of the extracted minutiae points of the fingerprint image.

A copyright protection scheme is proposed by Tu and Hsu [14] for digital images with multi-authorship. A visual secret scheme is used to split the ownership statement of "n" author's into "n" shares based on the features of the protected image. A logical OR operation is performed on ownership share of author and the feature map of the protected image to reveal the ownership statement. Shinde and Mohol [15] developed a copyright protection scheme for images on Android phones where bit plane complexity segmentation steganographic technique [16] is used which replaces the complex bits of bit plane of the color image which is difficult to detect by a human eye. Adelsbach *et al*. [17] developed an ownership proof scheme which uses a similarity test function both in the ownership proof and in the registration process, which helps to perform ownership proofs on similar works and also avoid multiple registrations of similar works.

Wang and Lin [18] developed a wavelet tree-based blind watermarking scheme for copyright protection by quantizing supertrees, which are the groups of wavelet coefficients of the host image. Each watermark bit is embedded in various frequency bands, and the information of the watermark bits are spread throughout large spatial regions. Ahmad and Lu [19] considered iris as the watermark. The features of iris are extracted using one-dimensional Gabor filters and then get encoded into bits using Daugman's four-level phase quantization. The cover image is transformed using wavelet transform, and the bit patterns are embedded in the transformed coefficients.

A perceptual watermark casting scheme is developed by Wang and Kuo [20] which searches the perceptual significant wavelet coefficients and the watermark is cast into selected significant coefficients to provide a higher level of tolerance against attacks. A multipurpose watermarking scheme is developed by Lu and Liao [21] which helps to achieve both authentication and protection of multimedia data for both image and audio watermarking. Instead of considering one watermarking scheme, their approach uses both robust watermarking and fragile watermarking. Huffman encoding [22], which is a variable length encoding method, is used by Nag *et al*. [23,24], to compress the payload to improve the embedding capacity. Kang and Aoki [25] developed a watermarking system, in which only the watermark data are transformed and embedded into untransformed cover image. A 2×2 submatrix is taken from the cover image by Ghoshal and Mandal [26] and transformed the submatrix into the frequency domain using Fourier transform, which results in real and imaginary part. Two bits of secret image are fabricated within the real part of each pixel, where the position is chosen using a hash function. The process is repeated for each submatrix to insert entire secret image bits.

MATRIX EMBEDDING

In the matrix embedding technique [27-32], "p" secret bits are embedded in 2^p-1 cover bits with at most one-bit change.

Embedding

Let x1, x2, and x3 be three least significant bits (LSBs) of a pixel of each channel which are treated as cover bits. To embed two bits, b1 and b2 in every channel of a pixel, exclusive OR (XOR) operation is done on the cover bits as shown in equations 1 and 2. The XOR operation outputs true only when inputs differ.

$$b1=x1 \oplus x2 \quad (1)$$

$$b2=x2 \oplus x3 \quad (2)$$

There are four different cases to be considered:

a. If Equation (1) is satisfied and Equation (2) is not satisfied, then flip x3
b. If Equation (1) is not satisfied and Equation (2) is satisfied, then flip x1
c. If both equations are satisfied, then no bit changes
d. If neither equation is satisfied, then flip x2.

Extraction

Three LSBs of each channel of a pixel are used to get two bits of secret data. To retrieve two bits, b1 and b2 from three cover bits: say x1, x2, and x3, equations 3 and 4 are applied.

$$b1=x1 \oplus x2 \quad (3)$$

$$b2=x2 \oplus x3 \quad (4)$$

These collected bit streams are combined to get the entire secret data.

PROPOSED WORK

Voluminous number of images and videos are stored in the networked computer on web. When some digital entity is online, there is a possibility that it is prone to theft. The notion of the proposed work is to uniquely identify a digital image along with real owner who had acquired the image. Even a theft of a very small fragment in the original digital image should be determined. This experiment is carried on the spatial domain of a raw image. The primary requirement of this biometric authentication (proposed work) is that the biometric trait, i.e., the image of owner's fingerprint has to be overlaid on each and every pixel of the original image. This is a challenge that has to be addressed because the uncompressed image size of fingerprint itself occupies one-quarter of the original image's file size.

The embedding model we want to adapt is invisible watermarking. Hence, to overlay the fingerprint image on the original image, a frame size or threshold is chosen for the original image. This frame size is the minimum pixel one should at least cut/remove from the original image to make a worthy stealing. Hence, it is finalized in the proposed work to lay the fingerprint image on every 8×8 blocks of the original image. However, in practical, a fingerprint image cannot be in the range of few bytes, say 100-200 bytes. Thus, the challenge is to scale down the fingerprint image to house it on every 8×8 blocks of original image. Naturally, this has become the requirement in giving authentication to the original image.

The fingerprint image of the owner is scaled down by hashing, which resulted in a unique 128-bit binary code. The matrix embedding technique used in the proposed work embeds two secret bits in every channel of a pixel (24 bits), which results in a need of 64 pixels to store the 128 bit hash code. In general, the size of the block is determined by the number of bits to be embedded. Hence, the cover image is partitioned into 8×8 non-overlapping blocks, and the hash code is embedded into every block. It is carried out in all the channels (RGB). Matrix embedding technique will bring less distortion to the original image during the process of embedding the 128-bit hash code on it. To prove the ownership of the image acquired by the owner, the following steps are carried out in embedding, extraction, and verification process.

Embedding process

Embedding operation is carried out in the spatial domain of the original image and is shown in Fig. 1.

1. Take the fingerprint image of the owner (from stored database); it may be in jpeg format. Hash the image and obtain 128-bit hash code

using Message Digest 5 algorithm [33].
2. Take the original photograph/snap, for which ownership has to be proven; this may be a raw 24-bit image (RGB); partition the image into multiple 8×8 non-overlapping blocks on all the channels (RGB).
3. The 128-bit hash code is embedded into every 8×8 blocks of original image on all the three channels through matrix embedding technique as discussed in section III.
4. Finally, an original image with fingerprint embossed authenticated image is created using embedding process.

Extraction process

The extraction process is carried out in the spatial domain from the embedded image and is shown in Fig. 2.

1. Take the suspected partial/fully stolen image, partition the image into multiple 8×8 non-overlapping blocks
2. Three bits from every pixel of 8×8 block is considered to get two secret bits through matrix extraction technique; this process is applicable for all the channels (RGB)
3. Using the collected bits, construct and build a 128-bit hash code. Do the same for every 8×8 blocks of original image.

Verification process

1. From the database, pull down the respective fingerprint image's hash code of the owner; which is a 128-bit hash code
2. Compare the extracted hash code with the database hash code; if the database hash code match with all the 8×8 blocks of the suspected image, then it is concluded that the image is stolen completely. Else if, it matches with only a few 8×8 blocks of the suspected image, then it can be concluded that partial theft of the original image has been attempted. Three different cases are considered in the verification phase.
   a. Image fully stolen: The number of blocks matched will be equal to the total number of blocks
   b. Image partially stolen: It occurs when a part of the image is stolen and if so, it identifies the matched blocks
   c. Image not stolen: The number of blocks matched will be equal to zero.

EXPERIMENTAL RESULTS AND DISCUSSION

In this section, the tests are done on images taken from LIVE database [34] as the cover images and images taken from CASIA fingerprint database for testing version 1.0 [35] as secret image to verify the validity of the proposed work. 25 out of 29 high-resolution reference images in the LIVE database are used for testing. CASIA-Fingerprint V1 database consists of 20,000 fingerprint images of 4000 fingers from 500 subjects.

Block matching

While considering three different cases for verification, the number of blocks matched varies. The number of blocks matched helps to identify whether the image is completely stolen, partially stolen or not stolen. For a fully stolen image, the number of blocks matched is same as the total number of blocks in the image. The number of matched blocks will be zero if the image is not stolen. For a partially stolen image, matched blocks are identified. Tables 1 and 2 show how many blocks are matched with the cover image in the case of fully stolen and partially stolen images, respectively.

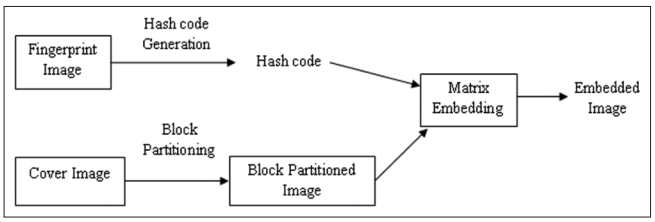

Fig. 1: Embedding process

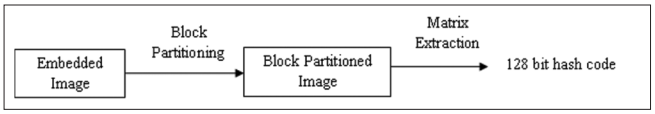

Fig. 2: Extraction process

Image quality assessment

Four objective image quality assessment metrics such as peak signal-to-noise ratio (PSNR), mean square error (MSE), structural similarity index (SSIM), and normalized cross-correlation (NCC) are used to find the similarity between cover image and the embedded image.

MSE

MSE is one of the simplest quality metrics to find the similarity between two images [36].

$$MSE=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(A(i,j)-B(i,j))^2 \quad (5)$$

Where A is the cover image and B is the embedded image. M×N represents the size of the image.

PSNR

PSNR [37] is an objective image quality assessment metric used to find the similarity between two images, which is measured in decibels (dB).

$$PSNR = 20\log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \quad (6)$$

SSIM

The SSIM index [38] is an efficient metric for full reference image quality assessments, in which similarity between two images is calculated by considering luminance, contrast, and structure. Given two images, X and Y of size M×N. Let μ_x, μ_y denote the mean of x and y, respectively, σ_x^2, σ_y^2 denote the variance of x and y, and σ_{xy} denote the covariance of x and y. The SSIM index between x and y is:

Table 1: Block matching - for fully stolen image

S.No.	Test image (.bmp)	Image size	Total number of blocks	Number of blocks matched
1	House	768×512	6144	6144
2	Sailing	480×720	5400	5400
3	Building	640×512	5120	5120
4	Parrots	768×512	6144	6144
5	Dolls	608×488	4636	4636

Table 2: Block matching - for partially stolen image

S.No.	Test image (.bmp)	Image size	Total number of blocks	Number of blocks matched	Matched blocks
1	House	768×512	6144	4	1, 2, 6, 9
2	Sailing	480×720	5400	4	13, 246, 426, 602
3	Building	640×512	5120	6	13, 326, 413, 566, 802, 813
4	Parrots	768×512	6144	3	385, 678, 962
5	Dolls	608×488	4636	1	772

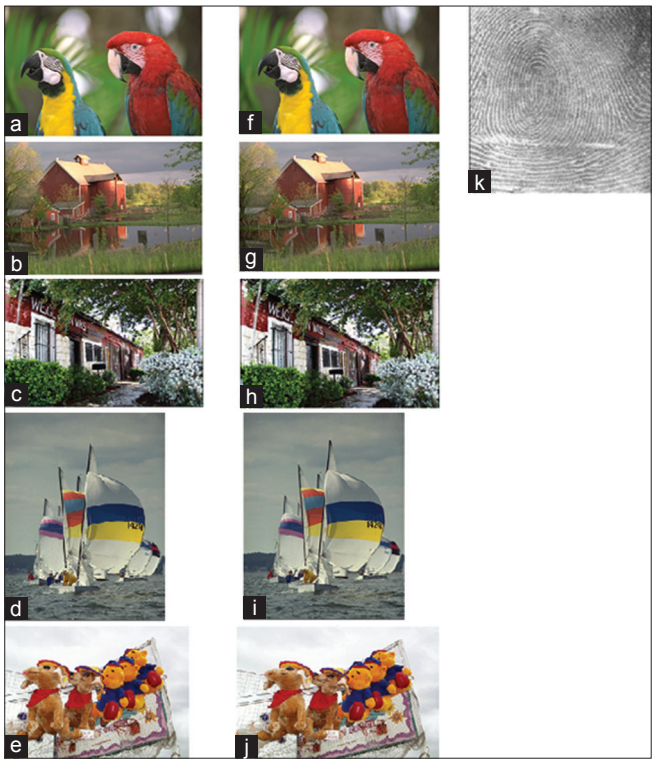

Fig. 3: Sample cover and embedded images, (a-e) Cover images, (f-j) embedded images, (k) authentic biometric image

Table 3: MSE, PSNR, SSIM and NCC- A comparison

S.No.	Test image (.bmp)	MSE	PSNR	SSIM	NCC
1	House	0.43	51.78	0.9840	0.9999
2	Parrots	0.48	51.82	0.9740	0.9999
3	Sailing	0.411	51.99	0.9768	0.9995
4	Building	0.427	51.83	0.9960	0.9997
5	Dolls	0.408	52.03	0.9810	0.9994

PSNR: Peak signal to noise ratio, MSE: Mean square error, SSIM: Structural similarity index NCC: Normalized cross-correlation

$$SSIM(x,y)=\frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)} \quad (7)$$

A n×n circular symmetric Gaussian weighting function [39] is used to modify μ_x, μ_y, σ_x, σ_y, σ_{xy}. The quality maps exhibit a locally isotropic property with a windowing approach. The overall quality of the image is calculated as the mean of the SSIM index of all windows.

$$SSIM(X,Y)=\frac{1}{P}\sum_{i=1}^{P}SSIM(x_i,y_i) \quad (8)$$

Where, P represents the number of sliding windows of the Image, X and Y are cover and embedded images, respectively, x_i and y_i are the image contents at the i^{th} local window. Its dynamic range is [−1, 1] and the best value of 1 is achieved if and only if both images are same. This method, based on the structural information of the image, has proved to be a good measure for very different kinds of images.

NCC

NCC [40] is used to find similarities between any two images E and C, respectively, and is given by:

$$NCC=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(C_{ij}\times E_{ij})}{\sum_{i=1}^{M}\sum_{j=1}^{N}(C_{ij})^2} \quad (9)$$

Fig. 3 shows the sample cover and embedded images. A comparison of various image quality metrics for assessing the quality between cover and embedded images for fully stolen case are given in Table 3.

LIMITATIONS

There are few limitations in the proposed work. It uses 8×8 sized blocks from the cover image to embed fingerprint image on it. There is a possibility that a small fragment of fingerprint embossed original image with less than 8×8 size could be stolen. However, in practical, this tiny stolen part does not give any significant details of an image. Furthermore, it is probable that part of an image could be stolen from inter-block pixels both in horizontal or vertical directions. If this activity is success and meaningful, then these types of theft remain undetectable.

CONCLUSION

In the proposed work, the owner's fingerprint is used as an invisible watermark, which uniquely identifies the owner of the image. Our work also identifies whether the image is completely or partially stolen and determines the blocks which are stolen too. The proposed method can be extended to support embedding in the frequency domain. Implementation is carried out on raw (bmp) images; this can be extended to other image formats as well.

ACKNOWLEDGMENT

The work is supported by Chavali and Appalaghe [41] Rashonic Unicpixel Technology Pvt. Ltd, Hyderabad, Telengana, India.

REFERENCES

1. Al-Nu'aimi A. Using watermarking techniques to prove rightful ownership of web images. 2013; p. 130-2. DOI: 10.4018/978-1-4666-2157-2.ch008.
2. Sencar HT, Memon N. Watermarking and Ownership Problem: A Revisit. 5th ACM Workshop on Digital Rights Management; 2005. p. 93-101.
3. Mali K, Bhattacharya S. Comparative study of different biometric features. Int J Adv Res Comput Commun Eng 2013;2(7):2776-84.
4. Davies J, Hare J, Samangooei S, Preston J, Jain N, Dupplaw D. Identifying Geographic Location of an Image with a Multimodal Probability Density Function. MediaEval Workshop; 2013.
5. Hsieh SL, Huang HC, Tsai IJ. A copyright protection scheme for gray level images using human fingerprint images as watermarks. In: Proceedings of the International Conference on Information Technology, New Generations; 2006.
6. Wang Y, Doherty JF, van Dyck RE. A watermarking algorithm for fingerprinting intelligence images. In: Proceedings of the Conference on Information Sciences and Systems; 2001.
7. Alomari R, Al-Jaber A. A fragile watermarking algorithm for content authentication. Int J Comput Inf Sci 2004;2(1):27-37.
8. Gunsel B, Uludag U, Tekalp AM. Robust watermarking of fingerprint images. Pattern Recognit 2002;35(12):2739-47.
9. Jain S. Digital Watermarking Techniques: A Case Study in Fingerprints and Faces, ICVGIP; 2000. p. 139-44.
10. Wu M, Liu B. Watermarking for image authentication. In: Proceedings IEEE International Conference on Image Processing. Vol. 2; 1998. p. 437-41.
11. Friedman GL. The trustworthy digital camera: Restoring credibility to the

photographic image. IEEE Trans Consum Electron 1993;39(4):905-10.
12. Saxena R, Shah K, Chawla R, Santhi V. Biometric watermarking for copyright protection of digital images. Int J Appl Eng Res 2014;9(24):23681-8.
13. Rao NN, Thrimurthy P, Babu R. An efficient copyright protection scheme for digital images using biometrics and watermarking. International Conference on Computer Science and Information Technology; 2009.
14. Tu SF, Hsu CS. A joint ownership protection scheme for digital images based on visual cryptography. Int Arab J Inf Technol 2012;9(3):276-83.
15. Shinde P, Mohol C. Copyright protection for images on android phones. Int J Res Eng Technol 2013;2(11):96-8.
16. Beaullieu S, Crissey J, Smith I. BPCS Steganography. San Antonio: University of Texas at San Antonio. 2003.
17. Adelsbach A, Pfitzmann B, Sadeghi A. Proving Ownership of Digital Content. Vol. 1768. IHW; 2000. p. 126-41.
18. Wang S, Lin Y. Wavelet tree quantization for copyright protection watermarking. IEEE Trans Image Process 2004;13(2):154-65.
19. Ahmad S, Lu ZM. A joint biometrics and watermarking based framework for fingerprinting, copyright protection, proof of ownership, and security applications. International Conference on Computational Intelligence and Security Workshops; 2007.
20. Wang HJ, Kuo CJ. Image Protection via Watermarking on Perceptually Significant Wavelet Coefficients. IEEE Workshop on Multimedia Signal Processing; 1998.
21. Lu CS, Liao HY. Multipurpose watermarking for image authentication and protection. IEEE Trans Image Process 2001;10(10):1579-92.
22. Huffman D. A method for the construction of minimum redundancy codes. Proc Inst Radio Eng 1952;40(9):1098-101.
23. Nag A, Biswas S, Sarkar D, Sarkar PP. A novel technique for image steganography based on block-DCT and huffman encoding. Int J Comput Sci Inf Technol 2010;2(3):103-12.
24. Nag A, Biswas S, Sarkar D, Sarkar PP. A novel technique for image steganography based on DWT and huffman encoding. Int J Comput Sci Secur 2011;4(6):561-70.
25. Kang S, Aoki Y. Image data embedding system for watermarking using fresnel transform. IEEE Int Conf Multimed Comput Syst 1999;1:885-9.
26. Ghoshal N, Mandal JK. A novel technique for image authentication in frequency domain using discrete fourier transformation technique. Malays J Comput Sci 2008;21(1):24-32.
27. Cox IJ, Miller ML, Bloom JA, Fridrich J, Kalker T. Digital Watermarking and Steganography. 2nd ed. Burlington: Morgan Kaufmann; 2008.
28. Sarkar A, Madhow U, Manjunath BS. Matrix embedding with pseudorandom coefficient selection and error correction for robust and secure steganography. IEEE Trans Inf Forensic Secur 2010;5(2):225-39.
29. Nithyanandam P, Ravichandran T, Priyadharshini E, Santron NM. A spatial domain image steganography technique based on matrix embedding and huffman encoding. Int J Comput Sci Secur IJCSS 2011;5(5):456-68.
30. Nithyanandam P, Ravichandran T, Priyadharshini E, Santron NM. An image steganography for color images using lossless compression technique. Int J Comput Sci Eng 2012;7(3):194-205.
31. Nithyanandam P, Ravichandran T, Priyadharshini E, Santron NM. An image steganography technique on spatial domain using matrix and LSB embedding based on huffman encoding. Imanagers J Future Eng Technol 2011;6(3):2011.
32. Nithyanandam P, Ravichandran T. A hybrid embedded steganography technique: Optimum pixel method and matrix embedding. In: Proceeding of International Conference on Advances in Computing, Communications and Informatics; 2012. p. 1123-30.
33. Rivest R. The MD5 Message Digest Algorithm, RFC 1321. Internet Engineering Task Force (IETF) published RFC1321: MIT Laboratory of Computer Science & RSA Data Security, Inc.; 1992.
34. Sheikh HR, Wang Z, Cormack L, Bovik AC. LIVE Image Quality Assessment Database Release 2. Available from: http://www.live.ece.utexas.edu/research/quality. [Last accessed on 2017 Feb 02].
35. CASIA-Fingerprint Image Database for Testing Version 1.0. Available from: http://www.biometrics.idealtest.org. [Last accessed on 2017 Feb 02].
36. Wang Z, Bovik AC. Mean squared error: Love it or leave it? A new look at signal fidelity measures. IEEE Signal Process Mag 2009;6(1):98-117.
37. Hmood KA, Kasirun ZM, Jalab AH, Alam GM, Zaidan AA, Zaidan BB. On the accuracy of hiding information metrics: Counterfeit protection for education and important certificates. Int J Phys Sci 2010;5(7):1054-62.
38. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP. Image quality assessment: From error visibility to structural similarity. IEEE Trans Image Process 2004;13(4):600-12.
39. Gonzalez RC, Woods RE. Digital Image Processing. 2nd ed. Upper Saddle River, NJ: Pearson Prentice Hall; 2002.
40. Sahu D, Parsai MP. Different image fusion techniques: A critical review. Int J Mod Eng Res 2012;2(5):4298-301.
41. Chavali R, Appalaghe AK. A System and method to identify a user using an imaging system. 5831/CHE/2014, 09/01/2015.