ISSN 22773061

A Spatial Domain Approach of Fingerprinting for Colored Digital Images

Vineet Mehan, Renu Dhir, Y. S. Brar
Department of CSE, NIT, Jalandhar
mehanvineet@gmail.com
Department of CSE, NIT, Jalandhar
dhirr@nitj.ac.inl
Department of EE, GNE, Ludhiana
braryadwinder@yahoo.co.in

ABSTRACT

In this paper, a spatial domain approach of fingerprinting is presented for colored digital images. A semi-blind fingerprinting conveys a secure arrangement for trading of digital images. The operational significance of the digital fingerprinting system is verified and estimated. Digital fingerprint implanted doesn't disturb the perceptible feature of the host digital image. Multi-user collusion attacks are prevented using the proposed apparoach. Variable fingerprint size and dissimilar location insertion play significant role for inhibiting attack.

Indexing terms/Keywords

Fingerrpinting, Colored digital images, Semi-Blind, Collusion Attack.

Academic Discipline And Sub-Disciplines

Computer Science Engineering

SUBJECT CLASSIFICATION

Digital Image Processing

TYPE (METHOD/APPROACH)

Fingerprinting

Council for Innovative Research
Peer Review Research Publishing System
Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY
Vol 11, No. 1
editor@cirworld.com
www.cirworld.com, member.cirworld.com

1 INTRODUCTION

Request for shielding intellectual possession of digital content is augmenting due to rise in crime escalation. The rise is allied with a prompt expansion of information technology and its organization. In fact, a massive amount of digital content have been copied. Digital fingerprinting using watermarking technique is one of the effective methods to defend digital content for content exchange.

Fingerprinting is a system that is castoff for finding illegitimate manipulators [1]. In this modus operandi, a unique identification number is inserted into content afore delivery. The identification number is called fingerprint. When a doubtful replica of the content is instituted, an owner can ascertain an illicit user by mining the fingerprint.

The digital fingerprinting lay emphasis on its distinctiveness of expedient locating. Contrary to it, the digital watermarking commonly upkeeps robustness of its watermarks for ascertaining the ownership [2]. Conferring to the utility of fingerprint, the digital fingerprint model prerequisites features [3] which includes: Transparency, Imperceptibility and Reliability.

The rest of this paper is structured as follows. In Section 2, literarte review related with the given work is stated. Section3 brings together the secure fingerprint implanting and retrieving system. In Section 4, emperimental results and discussions are presented. Finally the concluding remarks are given in Section 5.

2 LITERATURE REVIEW

A small and protected fingerprinting code for images is proposed by Kim and Suh [4]. An extension applied to the concept of watermarking is labelled as fingerprinting. In fingerprinting the distinctiveness of buyer is implanted into the digital image. The chief dissimilarity amongst watermarking and fingerprinting is that, in watermarking the mark is alike for all customers but for fingerprinting the mark is different every time. Fingerprint hinges on the buyer's uniqueness. The proprietor of digital image can trace the starting point of illegitimate copy by mining the buyer's identity. Attackers can scrap the fingerprint by equating different fingerprint images. This will aid attackers in locating the marks present. Attacks so tossed are termed collusion attack. Collusion attacks are prevented in this approach by varying the size of the fingerprint code in quotient to the number of customers.

A digital watermarking scheme based on composite watermarking is proposed by Chang et al. [5]. In this approach a new robustness improvement retrieval technique is presented by overlaying a number of weighted copies of condensed size watermark. Composite watermark is generated by decreasing the original watermark and then replicating it t times. Generated composite watermark is then encrypted and inserted into the original cover image.

Lee and Yoon [6] proposed a scheme of amalgamation amid Digital Rights Management (DRM) and fingerprinting. DRM organisation is liable for the protected delivery of the digital content. DRM averts the piracy of the digital content by means of encryption, but does not provide solution if encrypted content is hacked. Fingerprinting scheme is thus added to the DRM arrangement. Fingerprinting ensures identifying the illicit supplier of the digital content. In this paper a method for effective coordination is proposed that interconnect fingerprinting scheme with DRM structure. In order to affirm sufficient number of the users fingerprint length is set to 64-bits.

Swaminathan et al. [7] proposed a model for estimation of fingerprints. The paper classified fingerprints into two categories: intrinsic and extrinsic. Intrinsic fingerprints are generated using in-camera processing setups. Extrinsic fingerprints are inserted at the time of formation of multimedia data. Forensic signal processing procedures confirmed the presence and absence of intrinsic fingerprint in host image. A good correspondence among targeted coefficients resembles no alterations and confirms the integrity of the host image.

The problem of fingerprinting compressed signals is determined by Varna et al. [8]. The paper provides a solution to the collusion attack by designing collusion-resistant fingerprints. Fingerprinting scheme inserts fingerprint in each legitimately circulated copy of the image that distinctively ascertains the inheritor. When an unlicensed copy is revealed, the implanted fingerprint can be dig out and used to detect the basis of the leak. Several malicious consumers may work together by matching versions and form strong collusion attacks contrary to the fingerprinting scheme. Anti-Collusion Dither (ACD) is inserted to the compressed cover image so as to make the cover image more continuous and thus prevent the collusion attack.

A buyer-seller protocol is designed by Rial et al. [9]. The protocol is secret as the identity of the buyers is undisclosed. The protocol applies dual cryptographic primitives which include: group signatures and homomorphic encryption. Group signatures permit buyers to sign the acquisition media on behalf of group of buyers. The system is dynamic as new members can be added to the group easily. Homomorphic encryption lets buyer and seller to cooperatively work on encrypted watermark to be inserted in the host image. Adopting homomorphic encryption prevents the communicating parties to know the actual content of the watermark.

A content-based image fingerprinting mechanism is proposed by Lv and Wang [10]. Fingerprint is created by hashing the image. Within the image the shape contexts are identified using local feature points. Shape context descriptors generate the image hash value. Instead of embedding fingerprint in the image a separate database is maintained for storing the image hash.

3 METHODOLOGY

To identify each listed buyer and collusion attackers of a number of listed users, dissimilar size digital fingerprint is set into the identical digital image for all legal listed buyers. When the owner of the digital image catches some illegitimate

duplicates of the digital image on the Internet, he can find out the illicit liberators and take legal action for their unlawful plagiarize acts.

3.1 Fingerprint Embedding Algorithm

The key phases for embedding digital fingerprint are as follws:

1. Take a M × N colored digital image with a call for copyright fortification.
2. Read the two-dimensional pixel matrix of the digital image.
3. Genrate variable size fingerprint of buyer statistical data.
4. Split the host image into blocks of 4x4 dimensions.
5. Divide the number of blocks with the fingerprint size.
6. Calculate the number of blocks required for embedding the fingerprint.
7. Embed the fingerprint by relating XOR of blue color channel with the fingerprint
8. Save the manipulation to generate an output fingerprint image.

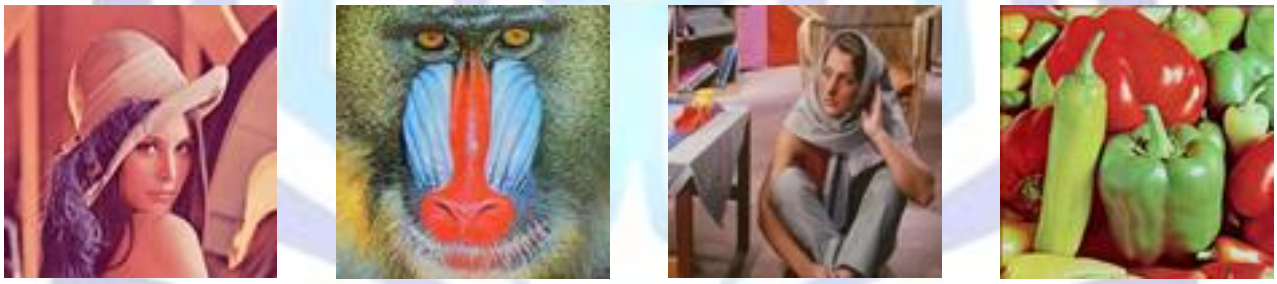
3.2 Fingerprint Extraction Algorithm

The key phases for ectracting digital fingerprint are as follws:

1. Take a M × N colored fingerprint digital image.
2. Read the two-dimensional pixel matrix of the digital image.
3. Split the host image into blocks of 4x4 dimensions.
4. Indentify the number of blocks containing the fingerprint.
5. Retrieve the fingerprint by relating XOR of blue color channel with the original fingerprint.
6. The extracted fingerprint is the same as original embedded fingerprint.

4 EXPERIMENTAL RESULTS AND DISCUSSION

Few original images for embedding fingerprint are shown in Fig 1. The resultant fingerprint images obtained after appling the embedding algorithm are shown in Fig.2.



(a) Image1 (b) Image2 (c) Image3 (d) Image4

Fig 1: Original Images

(a) Image1 (b) Image2 (c) Image3 (d) Image4

Fig 2: Fingerprint Images

Peak Signal to Noise Ratio (PSNR) is universally used quantity for defining the quality of images. PSNR calculates the peak signal to noise ratio amongst two images. The ratio factor is castoff for quality determination among host image and fingerprint image. In fingerprinting, a high value of PSNR denotes that the created image encompasses less noise. PSNR factor for diverse images with wavering fingerprint interval as shown in Fig3.

ISSN 22773061

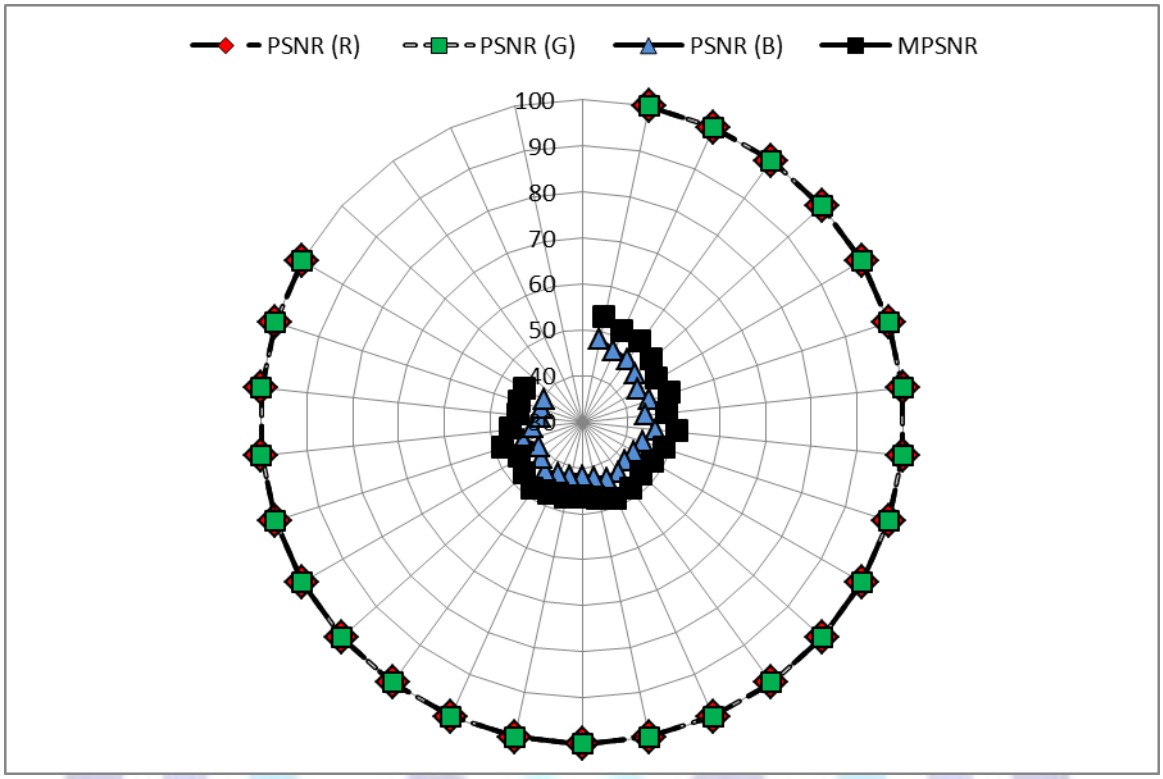


Fig 3: PSNR Analysis

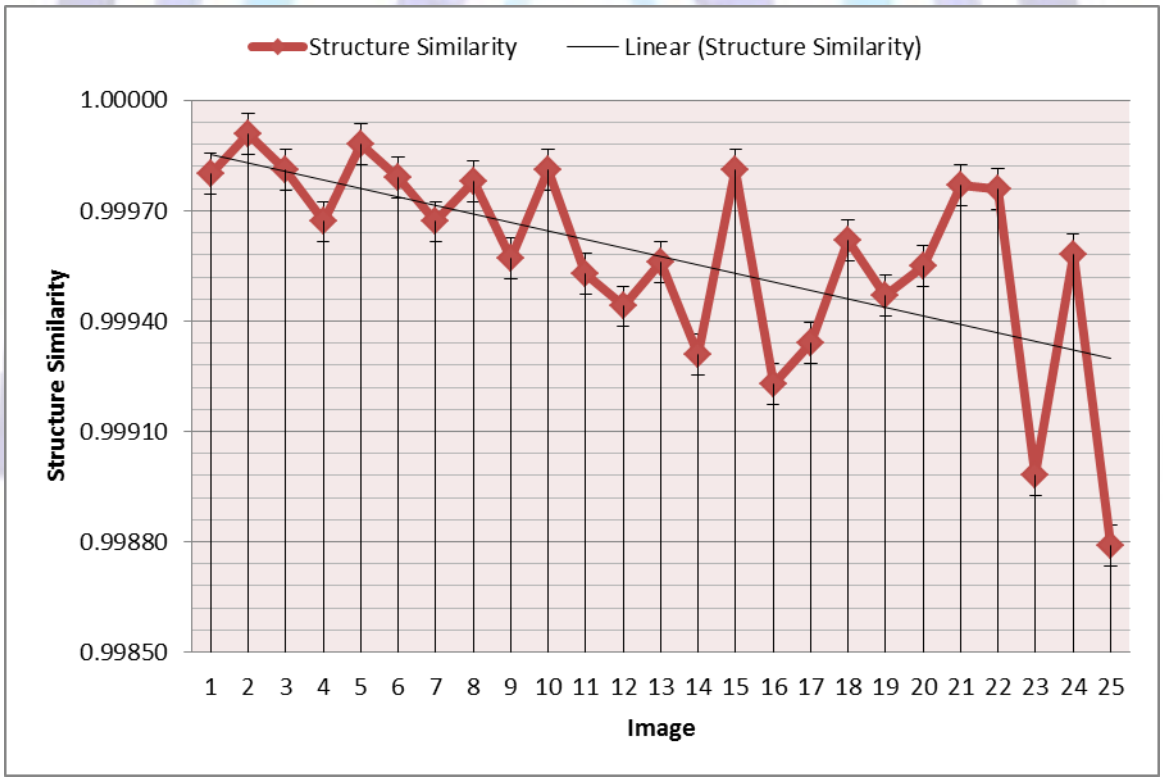


Fig 4: Structure Similarity Analysis

Structural similarity computes the correspondence amid two images. It is grounded on the concept of Human Visual System (HVS) that identify the distinction of structure amongst the original and the fingerprint image. Structural information existing in an image have sturdy inter-pixel enslavements amid spatial content. Similarity analysis for dissimilar images with changing fingerprint extent is shown in Fig 4.

5 CONCLUSION

In this paper, a fingerprint based image transmission system is presented with experimental results. The digital fingerprinting offers an effective tracing contrivance and protects the integrity of data for image electronic commerce system. Spatial domain approach of fingerprinting is achieved. Experimental outcomes deliver cogency of this scheme which is used for a image transmission under which user's message can be mined when pirated image is found. Colusion attacks are prevented successfully using this apparoach.

REFERENCES

[1] Min Wu , W. Trappe, Z. J. Wang, K.J.R. Liu, "Collusion-resistant fingerprinting for multimedia ", *IEEE Signal Processing*, vol. 21, pp. 15-17, 2004.

[2] Z. M. Lu and S. H. Sun, "Digital image watermarking technique based on vector quantisation," *Electronics Letters*, vol. 36, pp. 303-305, 2000.

[3] Voloshynovskiy, S, F. Farhadzadeh, O. Koval, O, "Active content fingerprinting: A marriage of digital watermarking and content fingerprinting", in *IEEE International Workshop on Information Forensics and Security (WIFS)*, 2012, pp. 175-180.

[4] W.-g. Kim and Y. Suh, "Short N-secure fingerprinting code for image," in *International Conference on Image Processing (ICIP)*, 2004, pp. 2167-2170.

[5] C.-H. Chang, Y. Zhi, and M. Zhang, "Fuzzy-ART based adaptive digital watermarking scheme," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 15, pp. 65-81, 2005.

[6] J.-S. Lee and K.-S. Yoon, "The system integration of DRM and fingerprinting," in *The 8th International Conference Advanced Communication Technology (ICACT)*, 2006, pp. 2180-2183.

[7] A. Swaminathan, M. Wu, and K. J. R. Liu, "Digital image forensics via intrinsic fingerprints," *IEEE Transactions on Information Forensics and Security,* vol. 3, pp. 101-117, 2008.

[8] A. L. Varna, S. He, A. Swaminathan, and M. Wu, "Fingerprinting Compressed Multimedia Signals," *IEEE Transactions on Information Forensics and Security*, vol. 4, pp. 330-345, 2009.

[9] A. Rial, M. Deng, T. Bianchi, A. Piva, and B. Preneel, "A Provably Secure Anonymous Buyer Seller Watermarking Protocol," *IEEE Transactions on Information Forensics and Security,* vol. 5, pp. 920-931, 2010.

[10] X. Lv and Z. J. Wang, "Perceptual Image Hashing Based on Shape Contexts and Local Feature Points," *IEEE Transactions on Information Forensics and Security,* vol. 7, pp. 1081-1093, 2012.

Author' biography

Vineet Mehan is with CSE Department at NIT, Jalandhar, Punjab, India. (e-mail: mehanvineet@gmail.com).

Renu Dhir is with CSE Department at NIT, Jalandhar, Punjab, India. (e-mail: dhirr@nitj.ac.in).

Yadwinder Singh Brar with EE Department at GNE, Ludhian, Punjab, India. (e-mail: braryadwinder@yahoo.co.in).