Volume 4, Issue 6, June 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Wavelet Coefficient Based Image Copy Detection and Privacy Preserving Using SIFT Attributes of Fingerprints

Miss. Payal R. Shete*
Department of Computer Science and Engineering,
Sinhagad college of engineering Vd. (Bk),
Pune, India.

Prof. Girija G. Chiddarwar
Department of Computer Science and Engineering,
Sinhagad college of engineering Vd. (Bk),
Pune, India.

Abstract— Recently, due to affordable price and easy operation on digital camera, large amount of digital images are available. In addition to that digital processing gives user privilege to modify the copy and spread the image over the internet. Digital multimedia, social networking and many more sites which deals with the images and that needs to be protected. To assure privacy of this storage there must be measures for copyright verification, image-content identification, copy detection, privacy and authentication perfectly. This architecture is proposed to solve the above problem of privacy of images. One way to solve it is to use the signs of Discrete Wavelet Transform (DWT) coefficients. The DWT based architecture allows searching images in the encrypted domain which is called as perceptual encryption. Sift attributes of fingerprints are used as input with the image to preserve privacy. The system will generates the set of two keys for scrambling of an image using sign component of low frequency wavelet coefficient which belongs to the particular image. Finally the statistical properties of these DWT sign vectors are modeled and focused on analyzing their robustness against real world image distortions.

Keywords— copyright, Content Based Image Copy Detection, Redundancy, SIFT.

I. INTRODUCTION

The success of the Internet and cost-effective digital storage device has made it possible to replicate, transmit, and distribute digital content in an effortless way. Thus, the protection of intellectual propertyright (IPR) has become a crucial legal issue. Detecting copies of digital media (images, audio and video) are a basic requirement for IPR protection (or copyright protection). The applications of copy detection include usage tracking and copyright violation enforcement. There are two approaches to protect copyright on the digital image, watermarking and content-based copy detection. Multimedia security [5] is the important term while dealing with the multimedia data. It is very necessary to ensure that, the data we are storing or using is secure. Multimedia security broadly falls into three categories [5]: first one is classical cryptography, second is watermarking and third is content fingerprinting.

Storing personal data on third party database servers gives rise to many privacy and security concerns. This necessitates the protection of data and the ability to process multimedia data in the protected domain efficiently. This requirement is fulfilled with the help of perceptual encryption, which significantly differs from the classical cryptography. The perceptual encryption is nothing but the addition of security measures to CBICD architecture and at the same time allowing for searching in copy detection domain.

The paper proposes the simple architecture for images based on signs of DWT coefficient [3]. In this architecture the vector of low frequency wavelet coefficients is used as an input in two functions. Firstly the vector gets expanded to form a key that drives the XOR based encryption. Secondly, it is used in a hash function which is used as a robust identifier in the database. The two main parts of the CBICD are database side and the query side. These two parts goes under the wavelet transform, in which the query side images are subjected to several common alterations in the CBICD framework

The rest of the paper is structured as follows. Section II explains literature survey. Section III is about design work and implementation details. Section IV explains the scale invariant feature transform. Remaining part shows result, conclusion and future scope.

II. LITERATURE SURVEY

Duplication and distribution of digital images can be accomplished in an effortless manner because of technological advancement in the last decade. Various alterations/attacks such as image scaling, compression, contrast and gamma changing and noise addition take place during the duplication and distribution process. As a result, one original image can have many copies with various alterations. This condition can harm the owner's rights of the images, if an efficient copy detection system is not available. An efficient copy detection method should have features that are robust to the attacks [3]. One solution to this problem is to use DWT transformations on Image.

Wavelet decomposition of the images is popularly used due to its inherent multiresolution characteristics. The core idea of using Discrete Wavelet Transform is to decrease/ reduce the size of the image at different level accordingly, for

example a square image of size $2^j \times 2^j$ pixels at level L is reduced to size $2^{j/2} \times 2^{j/2}$ pixels at level L+1. At every level, the image is decomposed into four sub images. The sub images are labeled LL, LH, HL and HH. LL represents the maximum energy coefficients or the approximation image. This image is used for further decomposition [11]. LH, HL and HH correspond to the vertical, horizontal and diagonal components of the particular image respectively. An example image along with its wavelet transform applied up to level 3 is shown in Figure 1.

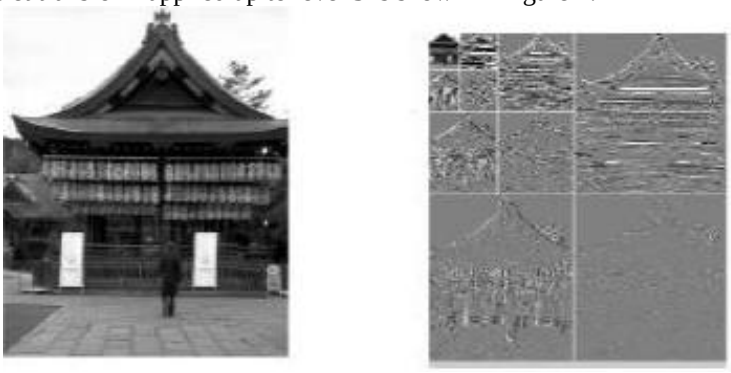


Fig. 1. An image and its Wavelet Transform [11]

Formula for DWT

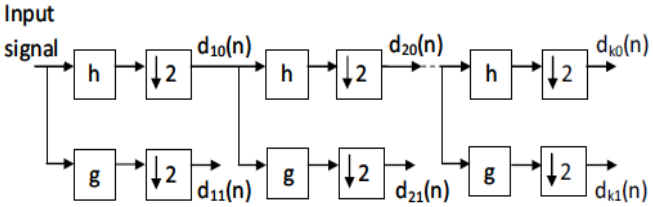
$$W_f(a,b) = \int_{-\infty}^{\infty} x(t)\Psi_{a,b}(t)dt$$

Formula for inverse DWT

$$x(t) = \frac{1}{C}\int_0^{\infty}\int_{-\infty}^{\infty} W_f(a,b))\Psi_{a,b}(t)db\frac{da}{a^2}$$

$$C = \int_{-\infty}^{\infty}\frac{|\Psi\omega|^2}{\omega}d\omega < \infty$$

These sub images can be combined together to restore the previous image which was decomposed. Due to this, DWTs are used for iterative comparison of matching blocks. The formula for DWT and inverse DWT are shown above which is applied on the image at the time of transformation. If the number of levels used for decomposition is L, then the matching performed on the LL image



- $d_{10}(n)$ lower band signal at level i.
- $d_{11}(n)$ higher band signal at level i.

Fig. 2. Low and High Pass Filter in DWT [3]

The wavelet provides many different capabilities like multi resolution, good energy compaction and adaptability to human visual system [3]. Wavelet transforms represent signal as a superposition of family of basis function called as wavelet [1]. The figure 2 represents the wavelet transform of the image where the input signal is passed to the low and high pass of the filter and output of that is again divided into two every time. The procedure is repeated until we get the several levels of decomposition as shown in the figure 1.

III. PROGRAM DESIGN

The basic architecture for image enrollment and copy detection is explained in the figure 3. Initially two inputs are given to the system the first one is the image for copy detection and the second one is the value of the attributes of fingerprint of the owner which is extracted from SIFT. The next step is to apply the DWT on the input image to convert it into the x (m) which contains the wavelet coefficient of that image. From this matrix the N × N top left, low frequency components are copied and removed, resulting in L = (N × N) elements. In matrix x(m), these N×N elements are then given a random sign [5][3]. The copied L low frequency components are binarized by the sign(.) Function, which represents a particular case of quantizer Q (.), As follows [6]:

bx(m) ={sign(x(m)[1]),....., sign(x(m)[L])}

Where for i ∈ 1,...,L , bx(m)[i]∈ 0, 1 and ∀ a, sign(a) = 1 if a ≥ 0 and 0, otherwise. The resulting binary vector bx(m) is used in two ways. This vector can also be called as a key which is very important because, firstly it serves as a seed for mapper that generates the matrix needed for the encryption. The encryption function E(.) Is a simple XOR against all wavelet coefficients, thus randomly flipping their signs. The main task of the mapper is to generate random pattern. The result (encrypted image and generated key) is stored in the database [6]. Secondly, bx(m) is hashed with cryptographic hash-function and an optional secret key k1 to form the database key belonging to this particular image entry m. Copy detection of a query image is done along similar lines. An image y is presented to the system. It is transformed by DWT to form DWT [3] coefficient matrix y. Again the N× N low frequency components are extracted, and (N×N) components are binarized to form by. Using the search procedure [4] number of candidate keys are generated from the Hamming sphere around by. Here this procedure is called as key reconciliation. The procedure works by simply flipping bits in the vector within a certain sphere bound, starting with the LRB (least reliable bit) first. All these combinations are hashed using hash function Ψ1(.).

The generated combinations are presented as a query to the database. If the perfect match is found the query side gives the encrypted DWT coefficients associated with that identifier in the database. Now the user uses his/her own vector by and mapper value to reconstruct the image and get the values of DWT [5] matrix back. The final image can then be obtained via the inverse DWT transform.

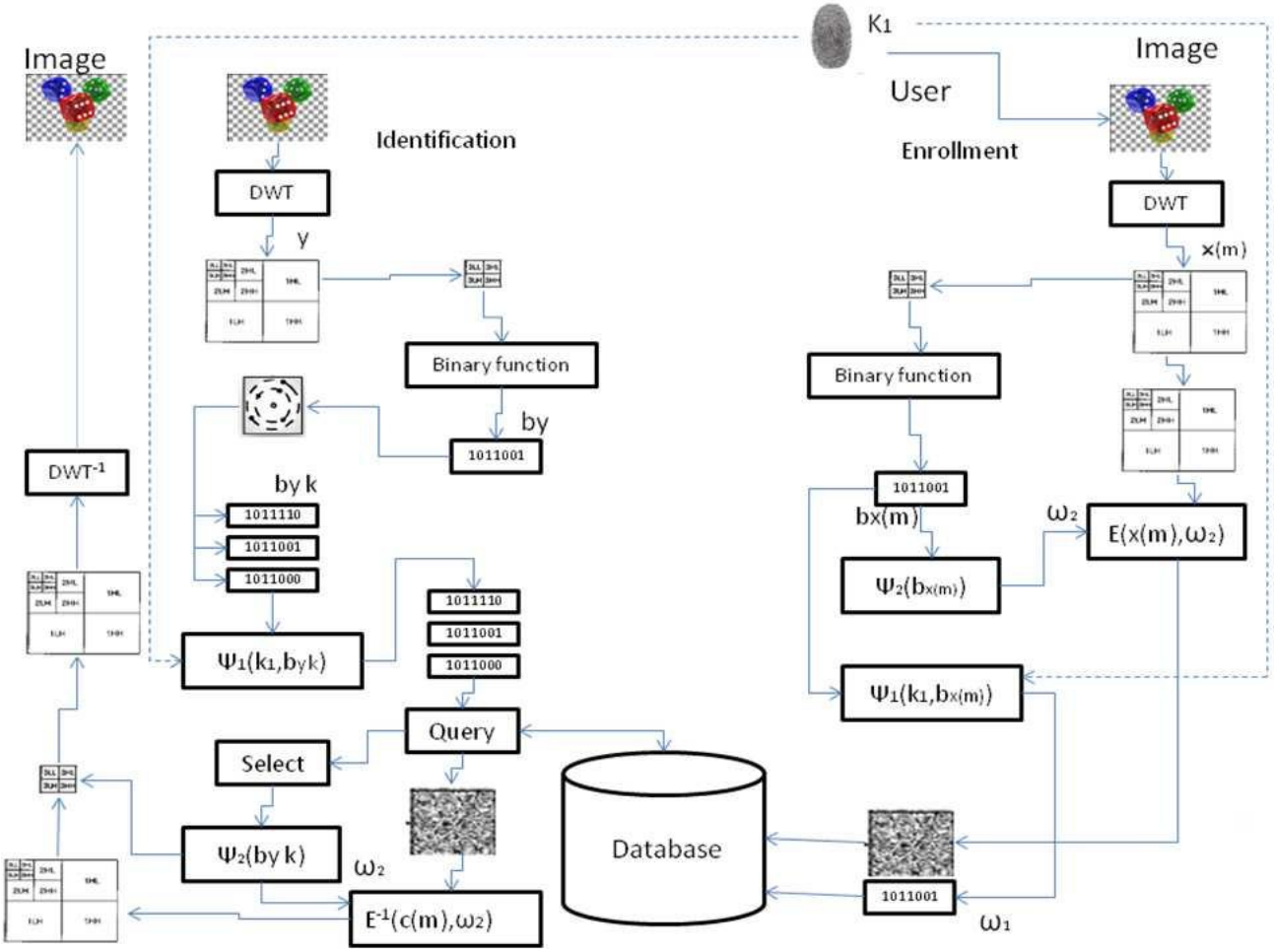


Fig..3 Proposed Architecture of Content Based Image Copy Detection

To increase security of image the concept of attributes of fingerprints are added into the architecture. The two way input submission of architecture will achieve higher reliability and provide more efficiency.

IV. SCALE INVARIANT FEATURE TRANSFORM

This section describes the concept of the Scale Invariant Transform Feature (SIFT) detector and descriptor. This method tries to extract an image from a collection of key points. SIFT is an approach for detecting and extracting local feature descriptors that are reasonably invariant to changes like illumination, image noise, rotation, scaling, and small changes in viewpoint. They are partially invariant to change of illumination as well. The core idea of SIFT is to remove the effect of such deformation using mapping activity among images which have the same elements. The SIFT descriptor is an important description of the edge found in the image, as they are the representation of key points and all their characteristics [13].

The figure 4 represents the different steps of SIFT model. The query image is passed from the following steps to extract the key point which is further used for matching purpose.

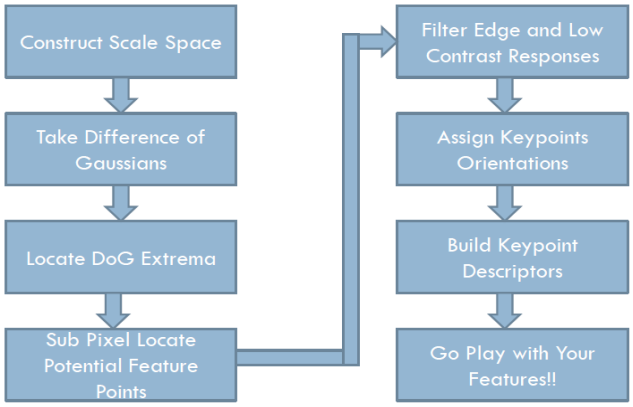


Fig. 4: Steps Of SIFT Algorithm

A. Sift On Fingerprint Images

In particular fingerprint image Minutiae points are strictly defined by the ridge ending and bifurcation points. So the number of minutiae points appearing in the image is bounded to a small number (<100). But if we take SIFT into the consideration points are only limited by the condition of local minima or maxima in a given scale space, resulting in a large number of feature points. The count of SIFT feature points depends on the set of parameters such as the number of octaves used in the procedure. Usually fingerprint image may contain up to a few thousand SIFT feature points. Fig. 4 shows an example of both minutiae points and SIFT feature points on the same fingerprint image. There are only 36 minutiae points, whereas the number of SIFT feature points is observed to be 2,020 which is quite a large number [12]. The SIFT parameter value used are the number of octaves = 4.

(A) 36 Minutiae Points (B) 2020 SIFT Feature Points

Fig. 5. Minutiae And SIFT Feature Points Extracted From The Same Image (A) Minutiae Points (B) SIFT Feature Points [12].

After getting the n number of SIFT feature points from the particular fingerprint image, we apply sorting on minima points to get the first 128 bits. This 128 points are used as the input to the system as the attributes of the fingerprints. For simplicity128 bit can be called as a key which is further used for various process in system architecture. The attributes of fingerprint used to achieve the higher level of security and privacy. The same procedure is repeated for the query side also and the results are extracted on the basis of matching of attributes of fingerprints. Figure 6 shows the approximate procedure of matching in two images referred from the literature survey paper.

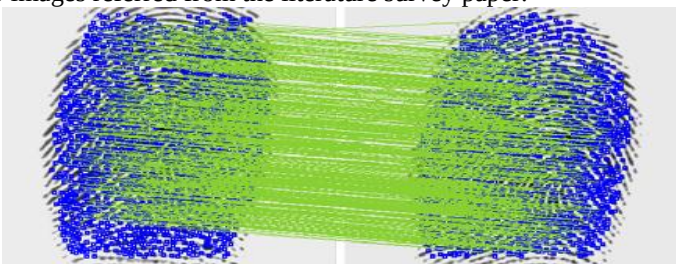


Fig. 6: Point Wise Matching [12]

V. RESULTS AND DISCUSSION

B. Data Set

The main goal of content based image copy detection system is to provide the original copy of the image stored in the database. The rich image database is necessary to recognize the copy of the query image from the no. of database images. The database contains the no. Of images, some of the images from the database are original and some images are added with prior modifications. These modifications are nothing but the different alteration made in the image. Gamma changing, contrast change, scale change, blur, rotation is few image alteration types. By using this type of alteration the no. of images are generated and all original and altered images are kept in the same database. Now this database is the main database for CBICD system. With the help of this database the two copies of the images (database side and query side) are getting detected.

B. Result Set

The system will result whether the two copies of the images are same or not. If the two copies are same then match found otherwise math does not exist message will get printed on the screen. From the literature survey following results are obtained. The paper uses the UCID [14] version 2 database (uncompressed color image database) which contains the 1088 colour images WITH 512 × 384 pixels (portrait and landscape orientation) and along with that different images with slight alteration.

C. Performance Metrics

To measure the performance of the detection metrics is used and that metrics is called as the recall and precision (R&P) let's consider the $n_{correct}$ and n_{miss} are the no. of correct and miss candidates[7]. The recall for particular query (q) image is defined as

$$call_q = \frac{n_{correct}}{n_{cor}Re_{rect} + n_{miss}}$$

Let n_{wrong} be the no. of wrongly retrieve images. Then the value of the precision for query image is defined as

$$Precision_q = \frac{n_{correct}}{n_{correct} + n_{wrong}}$$

VI. CONCLUSION

High discriminative power in the distortion free regime and degraded performance of query through some form of channel distortion are observed through binary vector. When attackers does a significant attack on image in form of information leakage, to recover from this attack high quality reconstruction of image is done. As per demonstration elaborated in literature survey this approach is infeasible.

Here DWT technique is used to search the identical image copies based on sign values of wavelet which overcomes the overhead associated with DCT. The SIFT attributes of fingerprints are used to preserve the owner privacy. A proposed framework uses this approach for effective identification of identical copies and provides significant level of security in terms of perceptual encryption.

REFERENCES

[1] Changick Kim, Content-based image copydetection, Signal Processing: Image Communication 18 169184 Epson Palo Alto Laboratory, Epson Research and Development Inc., 3145 Porter Dr. Suite 104, Palo Alto, CA 94304, USA 2003.

[2] F. Arnia, K. Munadi, M. Fujiyoshi, and H. Kiya, Efficient content-based copy detection using signs of dct coefficient, vol. 1, pp. 494 499, oct. 2009.

[3] Fitri arnia, agustinus Ifan, khairul munadi, Massaki fujiyoshi, hitoshi kia, Content based image copy detection based on sign of wavelet coefficient, International Workshop on Advanced Image Technology 2011 January 7-8, 2011

[4] F. Beekhof, S. Voloshynovskiy, O. Koval, and T. Holotyak, Fast identification algorithms for forensic applications, December 2006

[5] Handbook of image and video processing editor AL Bovik.

[6] M. Diephuis, S. Voloshynovskiy, O. Koval and F. Beekhof‟"DCT Sign Based Robust Privacy Preserving Image Copy Detection for Cloud- based Systems" Stochastic Information Processing Group, Universite de Gen‘eve 1227 Carouge, Switzerland Maurits 978-1-4673-2369-7/12 2012.

[7] Nadia Baaziz and Maxime Guinin, Content-Based Image Copy Detection Using Dual Signatures, 978-1-4673-0753 IEEE cole Nationale Suprieure dIngnierie de Caen (ENSICAEN), 14050 Cedex 04 France 2011.

[8] N. Ahmed, T. Natarajan, and K. Rao, Discrete cosine transform, Com- puters, IEEE Transactions on, vol. C- 23, no. 1, pp. 90 93, jan. 1974.

[9] "The Discrete Cosine Transform (DCT): Theory and Application1 Syed Ali Khayam Department of Electrical and Computer Engineering Michigan State University March 10th 2003

[10] Y. H. Wan, Q.L. Yuan, S.M. Ji, L.M. He,Y.L. Wang A survey of the image copy detection Zhejiang Province NSF Grant Y106332 IEEE Zhejiang University of Technology Hangzhou, China 2008.

[11] Saiqa khan, Arun Kulkarni, "Reduced Time Complexity for Detection of Copy- Move Forgery Using Discrete Wavelet Transform " International Journal of Computer Applications (0975 – 8887) Volume 6– No.7, September 2010

[12] Unsang Park, A. K. Jain, Sharath Pankanti,Dept. of Computer Science & Engineering, Michigan State Univ., East Lansing, MI, USA 48824,"Fingerprint Verification Using SIFT Features", SPIE Defense and Security Symposium, Orlando, Florida, 2008.

[13] An implementation of SIFT in Java code.

[14] G. Schaefer and M. Stich (2004) "UCID - An Uncompressed Colour Image Database", *Proc. SPIE, Storage and Retrieval Methods and Applications for Multimedia 2004*, pp. 472-480, San Jose, USA.

