Matching the Digital Image of the Dactylogram for a Secure Data Embedding Process using LSB and RNG

Renganathan. B, Saranya. M & Chinnadurai. S.

Srinivasan Engineering College, Perambalur, India
E-mail : its4renga@gmail.com, logon2saran@gmail.com, duchinna198227@gmail.com

***Abstract* – The overall problem digital image matching is managing a large Image database for storage and redundancy in matching methods. Digital image forensics was used for matching fingerprints. The system is not reliable and verifiable for the internet-based attacks. To overcome these aspects, LSB and RNG methods used to provide the expected results for accuracy and security. In the proposed, both Cryptography and steganography are used to provide security for matching methods. A severe Binary-Quantization concept is used to achieve accuracy and reduce time consuming for computational complexity Dactyl gram. The digital image of the finger print pattern is capture through the live scan and it provides a secure Internet voting service.**

Keywords – Biometric, Binary Quantization, cryptography, steganography, STEGO.

I. INTRODUCTION

Now days, the use of digital camera and the video equipped devices such as mobile phones tablets are used to create a escalating volume of images and videos, they were uploaded and shared among friends, while sharing the images needs to be stored managed they have to contented, evaluated and acquired. Even though the source of the captured image (camera, camcorder, cell phones) can be estimated by existing features, but in many issues such as terrorist related images were uploaded to the civilians' social network. In order to stop the illegal activities source identification of the digital image is done. Here the applications set for the biometric technologies. Biometric technologies use physical characteristics, such as voice tone or hand shape, to identify people automatically.

II. RELATED WORK

A common noise pattern to identify the original source of the sensor finger print is done by pattern noise in the image. The pattern noise present in the image is a PNU (Pixel Non Uniformity) noise is common noise pattern available in all digital imaging sensors (CMOS, CCD, Fovea™ X3,). The noise present in the image is found by correlation, the same used in identification of the spread spectrum watermark. The reliability of camera identification from images processed using JPEG compression gamma correction, and combination of JPEG compression and in-camera evaluated using FAR and FRR error rates. PNU is a pixel caused by different sensitivity of light. [1][5]There exist two basic components of the pattern noise are the Fixed Pattern Noise (FPN) and The Photo-Response Non-Uniformity noise (PRNU). The fixed pattern noise (FPN) is always caused by the dark currents. It is primarily refers to pixel-to-pixel differences when the sensor array is not exposed to light. Since the FPN is an additive noise, some middle to high end consumer cameras suppress this noise automatically by subtracting a dark frame from every image they take. FPN also depends on exposure and temperature.

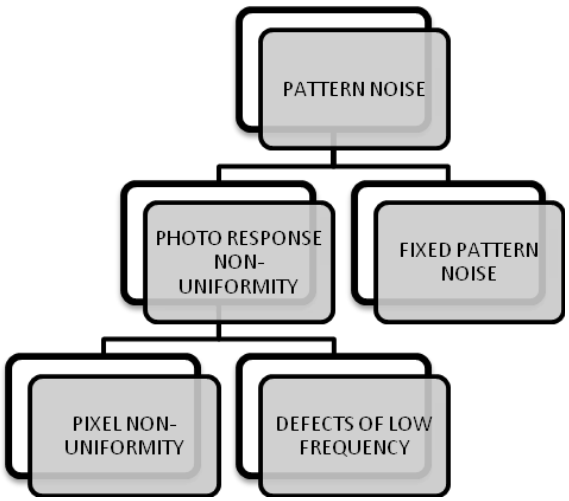

Fig 1. Hierarchy of Pattern noise

The digital camcorders use the same digital sensors. Each and every sensors use to link the digital camera images from various sources. The Photo Response Non uniformity noise pattern is used to identify the source Digital camera. The PRNU noise mentioned above have the characteristics to find the individual image sensor [6]. The PRNU noise is caused by the lights in sensor images due to variations in the individual pixels as a result of its sensitivity. The properties such as in homogeneity and impurities in silicon wafers and imperfections introduced by the sensor manufacturing process cause the pixel variation in the sensor images. The noise of the one image sensor can be matched with the noise of another one. This can be done by correlating factors of the two image sensor.

The dot product of I and J is

$$I \odot J = \sum_{i,j=1}^{(k,n)} I[x,y].J[x,y]$$

With I being the norm as shown $\|I\|=\sqrt{I \odot I}$

$$Corr\,(I,J) = \frac{(I-\bar{I}) \odot (J-\bar{J})}{\|I-I\| \odot \|J-J\|} \qquad (1)$$

The above equation is the correlation of image sensor of two images. Then the PRNUs are filtered to remove the blocking artifacts due to lossy compression. At last, they are processed using the normalized cross-correlation. The Peak to Correlation Energy coefficient is used to establish the common origin of both PRNUs. Experiments with 30 camcorders show that only 48 seconds of video is sufficient for a very reliable decision from clips encoded as low as 450kb/sec.

Fig. 2 : Palm based matching

Matching finger print is one of the well-known aspects in the Biometric techniques. Finger prints in application area is used for two purpose verification and identification. In verification, the input is a query fingerprint and an identity (ID), the system verifies whether the ID is consistent with the fingerprint. The output is an answer of yes or no. [4] In identification, the input is only a query fingerprint; the system tries to answer the question: Are there any fingerprints in the database that resemble the query fingerprint? The output is a short list of fingerprints.

The finger print is made up of End-points and bifurcation. End point in the finger print is the ending of the minutiae line. Bifurcation is just splitting of the line into branches. We can distinguish three main fingerprint matching techniques. The first technique is minutiae based matching. Minutiae are defined as the discontinuities of the ridges of the fingerprint.

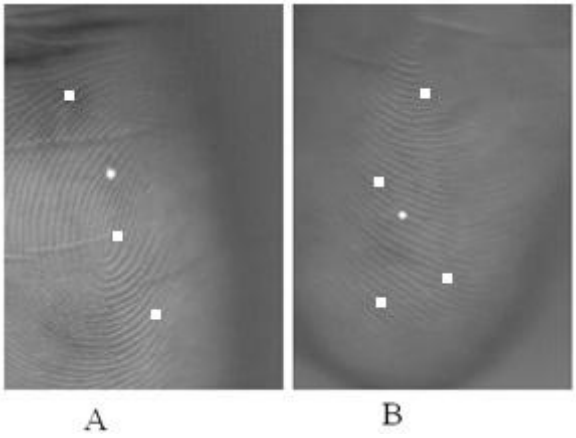

Fig 3. Regions Exposing

Given a fingerprint image, after appropriate image pre-processing, enhancement, segmentation, minutiae points can be extracted through different minutiae detection algorithm. The minutiae have two portions Endpoint [A] and Bifurcation [B] .Usually minutiae are represented by a tuple of values including its coordinates, the ridge direction and the type of endings. Through approaches of point pattern matching, minutia based matching can be implemented. Various Minutiae based matching systems have been developed.

III. TECHNIQUES

A. Severe Binary Quantization

A Binary- Quantized model consists of a set of binary feature vectors (square sub templates) arranged with respect to each other in image coordinates. Each model comes from a training image of the object in a known pose. We get binary edge images using dilated zero crossings of Laplacian of Gaussian versions of the training images. The Gaussian filter has $\sigma = 2$, and $n_d = 3$. The process is to help ensure some overlap between training features and possibly corrupted actual features. We designate the edge training images as

$e_i(x, y)$, where $i \in [1,2,3,\ldots,n_m]$ indexes the model and $x \in [0,1,2,3,\ldots,n_x - 1]$ and $y \in [0,1,2,3,\ldots,n_y - 1]$ give the pixel coordinates on the n_x x n_y image. We eliminate the background by making binary masks using backlighting. A model M_i represents features that are square patches of dilated edge points from $e_i(x, y)$. $D_H(\bar{r}, \bar{s})$ is the Hamming distance between binary vectors $\bar{r}$ and $\bar{s}$. The Hamming distance simply counts the number of unequal elements in corresponding positions of its two arguments. In words, $r_i(x, y)$ is computed by taking a square of dimension $(2b+1)$ x $(2b+1)$ pixels centred on (x, y) in $e_i(x, y)$ and computing its Hamming distance with equal sized squares of pixels centred in the surrounding d x d neighbourhood of $e_i(x, y)$. . The minimum of these Hamming distances is the rating of the feature. The feature will rate highly if it is dissimilar to its surroundings. Consider $b = 7$ pixels to give binary features of size 15x15. Consider $d = 3$ pixels. The best feature is taken as the $(2b+1)$ x $(2b+1)$ square surrounding the maximum value in $r_i(x, y)$. Subsequent features are chosen as squares surrounding the next highest value in $r_i(x, y)$ that does not overlap any previous features.

B. Cryptography and Steganography

1) Least Significant Bit: LSB (Least Significant Bit) substitution is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding message into the image. The Least Significant Bit insertion varies according to number of bits in an image. For an 8 bit image, the least significant bit i.e., the 8th bit of each byte of the image is changed to the bit of secret message. For 24 bit image, the colors of each component like RGB (red, green and blue) are changed. LSB is effective in using BMP images since the compression in BMP is lossless. But for hiding the secret message inside an image of BMP file using LSB algorithm it requires a large image which is used as a cover. LSB substitution is also possible for GIF formats, but the problem with the GIF image is whenever the least significant bit is changed the whole colour palette will be changed. The problem can be avoided by only using the gray scale GIF images since the gray scale image contains 256 shades and the changes will be done gradually so that it will be very hard to detect. For JPEG, the direct substitution of steganographic techniques is not Possible since it will use lossy compression. So it uses LSB substitution for embedding the data into images.

2) Random Number Generation: Random Number Generators (RNGs) used for cryptographic applications typically produce a sequence of zero and one bits that may be combined into sub-sequences or blocks of random numbers. There are two basic classes: deterministic and nondeterministic. A deterministic RNG consists of an algorithm that produces a sequence of bits from an initial value called a seed. A nondeterministic RNG produces output that is dependent on some unpredictable physical source that is outside human control. There are no FIPS Approved nondeterministic random number generators.

3) Triple DES Algorithm: In cryptography, Triple DES is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.

IV. EXPERIMENTS AND RESULTS

Accuracy Result: Each and every elements of the pixels in the digital image is correlated by the above features such as texture, ridges, Bifurcation present the sensor image. Here Each and every user was asked to provide 4 different impressions of each of 4 different fingers - the left index finger, the left middle finger, the right index finger and the right middle finger. A set of 6120 (170 ×6 × 6) images were collected. We compare this performance with a minutiae-based approach [6] that does not utilize texture information for representing the fingerprint. The hybrid approach outperforms the minutiae-based approach over a wide range of FAR values. For example, at a 1% FAR, the hybrid matcher gives a Genuine Accept Rate of 94% while the minutiae-based matcher gives a Genuine Accept Rate of 81%.

TABLE 1. Correlation between images

Images	1	2	3	4
Total Bifurcations	54	42	30	40
Total End points	26	22	36	12
Correlation Percentage	48%	42%	18%	30%

V. CONCLUSION AND FUTURE ENHANCEMENT

Sensor fingerprints are large in dimension and random in nature. Due to these characteristics, conventional fingerprint matching methods are not practical when large databases of fingerprints have to be searched. The main goal is to improve on existing matching methods by addressing more practical concerns like storage requirements and computation time while still maintaining an acceptable matching accuracy. In the proposed system to create a compact representation of fingerprints through quantization..The focus is on the most severe form of quantization and every element of sensor fingerprint is severely quantized into a single bit. After a successful matching of the fingerprint the user was allowed embed the data in a secure way. By using both cryptography and steganography at the same time, the data is embedded in a secured environment.

VI. REFERENCES

[1] Sevinç Bayram, Hüsrev Taha Sencar, and Nasir Memon, "Efficient Sensor Fingerprint Matching Through Fingerprint Binarization" IEEE transactions on information forensics and security, vol. 7, no. 4, august 2012

[2] Andreas Gutscher Jessica Heesen and Oliver Siemoneit, "Possibilities and Limitations of Modeling Trust and Reputation" IEEE transaction on System & Data reputation, 2002.

[3] Dirik, Yanmei Fang," Source Class Identification for DSLR and Compact Cameras" IEEE transaction on Information Forensics and Security vol 3: 3.2009.

[4] Eric Kee, Micah K. Johnson and Hany Farid,"Digital Image Authentication from JPEG Headers" IEEE transaction on Information Forensics and Security Vol 6:3 2011.

[5] Goljan.M, J. J. Fridrich, and T. Filler, "Managing a large database of camera fingerprints" IEEE Transactions on Information Security and Forensics vol 7:2, 2012.

[6] Jessica Fridrich, D.Soukal, Jan Lukáš, "Detection of Copy-Move Forgery in Digital Images",IEEE Transactions on Information Security and Forensics August 5-8 2003.

[7] Jessica Fridrich, and Miroslav Goljan, Determining Digital Image Origin Using Sensor Imperfections IEEE Transactions on Information Security and Forensics, 1(2), pp. 205-214, June 2006.

[8] Kurt Rosenfeld Taha Sencar Nasir Memon "A Study of the Robustness of PRNU-based Camera Identification" IEEE Transactions on Signal Processing, November 2002.

[9] Lars Hopland Nestås, Bouvet ASA, Norway Kjell J. Hole, "Building and Maintaining Trust in Internet Voting" IEEE Transactions on Vehicular Technology, March 2006.

[10] Mo Chen, Jessica Fridrich, "Source Digital Camcorder Identification Using Sensor Photo Response Non-Uniformity" IEEE Transactions on Information Security and Forensics, January 2007.

[11] Thomas Gloe," The'Dresden Image Database 'for Benchmarking Digital Image Forensics" IEEE Transactions on Information Security and Forensics vol 5:4, 2010.