Performance analysis of cancelable unimodal and Multiple biometric using distortion transformation algorithm

[1]N.Gomathy, [2]Dr.N.Radha
[1,2] *Department of computer science, PSGR Krishnammal College of arts and science, Coimbatore,* India.
gomathy789@gmail.com

Abstract

Objectives: Cancelable unimodal and Multiple Biometric Using Distortion Transformation Algorithm solve the problem of raucous data, non-universality and unacceptable error rate during authentication.
Methods: Distortion Transformation algorithm used for generate key from multiple biometrics.
Results: The cryptographic key generation of multiple finger print and palm print of the same person. It gives more authentications.
Conclusion: The features are extracted from the palm print and multiple finger print of same person. The extracted features are used to generate the key using distortion algorithms which are used for further authentication. This cryptographic key is stored in the database and used for verification process.

Index Terms: Security analysis, Palm print, Biometric system, Multiple Fingerprints, Fusion.

1. Introduction

Reliable authorization and authentication has developed an integral part of every man's life for a number of routine purposes [1]. Biometric technique used for recognizing a person based on physiological or behavioral features. This system considered as a reliable solution for protecting the identity and the human rights of individuals as it identify unique and immutable features. Biometrics is used for two authentication method**.**
Identification: This establishes a person's identity depends only on biometric determination.

Verification: It involves authenticating or denying a person's declared identity. A basic identity (e.g. password) is accepted and a biometric template of the subject is taken to match using a 1:1 matching technique to verify the person [2]. Biometric modalities commonly executed include fingerprint, face, iris, voice, vein pattern, and hand geometry. A lot of modalities are in different stages improvement and assessment. Biometric schemes are commonly used to organize the access to objective assets (laboratories, buildings, cash from ATMs, etc.) or logical information (personal computer accounts, secure electronic documents, etc). Biometric systems can also be used to measure whether or not a person is already in a database, such as for social service or national ID applications [3].

1.1 Structure of Biometrics system

Every biometric system consists of four basic modules. There is Enrollment center, Stored Templates, Sensor, Feature extraction, Matcher.

1.1.1 Enrollment

In that enrollment phase Individuals are registered into the system database. During this phase, the individual's biometric characteristics are scanned by biometric reader and to generate its digital representation.

1.1.2 Feature Extraction

This phase processes the input image to produce a compact symbol which is called as template. That can be stored in a essential database [4].

1.1.3 Matching

The matching unit compares the present input with the template. If the biometric system performs identity recognization, it matches to the novel characteristics to the user's master template and produces a score or match value [5]. The system doing identification competition a novel individuality against the master pattern of numerous users resulting in multiple match values.

1.1.4 Decision Maker

The decision maker unit accepts or discards the user depends on a security threshold level and matching level.

1.2 level of fusion

In recent decades, multiple and biometrics fusion methods have accomplished much focus of interest as additional information among diverse modalities that could improve the identification performance. The greater part of the works have focused on multimodal biometrics [6][7]. It is mainly classified into three main levels. They are

- Feature level fusion
- Match level fusion
- Decision level fusion

1.3 Fusion Prior to Matching

In this class, fusion method combines the information of biometric features before matching. This includes the following fusion levels.

Sensor level fusion

In this fusion process, without extraction of any feature the raw data obtained from the sensors are fused and denoted as a single unit. This type of fusion technique is called image level fusion or data level.

Feature level fusion

Data obtained from various sensors are first involved to feature extraction methods and the feature vector which is consequently used for identification.

1.4 Fusion after Matching

In this category, fusion integrates the information of biometric after matching. This includes the following fusion levels

Match-score level fusion

The Extracted Features from human biometric modalities are first matched to find the match scores. The scores obtained from various biometric systems are then joint to produce a fused match score.

Decision level fusion

Decisions of individual biometric classifiers are used to calculate a pooled decision. This level of fusion is called as abstract level fusion because it is used when there is access to only decision from entity classifiers.

Rank level fusion

Rank level fusion engrosses joints the identification rank achieved from numerous unimodal biometrics. It merges the rank that is used for final decision.

Related work

Nazmeen Bibi Boodoo and R K Subramanian [8] mined the features of ear and face by PCA method then fused the features at decision level by AND rule, enhanced the accuracy of recognization method, as well as decrease the FAR to 0%. But fusion at decision level and score level utilize only less information from the biometric for recognization.

Tulyakoy et. al[9] presented a hash-based transformation technique for secured template production. For each minutia, the N nearest neighbor minutiae was found and M (MoN) hashed minutiae were produced by using symmetric hash functions. The hashed minutiae points in the system database are matched with query hashed minutiae points. These hash functions having the good biometric properties. However, they did not explain how the recently hashed minutiae could be produced when stored minutiae were cooperated.

Chulhan et. al [10] presented a method for producing cancelable fingerprint templates that do not need alignment and a method for structure changing functions. By mining translation and invariant function value from each and every minutia, cancelable patterns of fingerprints are created. After that the conversion and movement direction of each minutia is determined by using two changing functions. Each minutia is turned and moved by the transformed minutia by means of the direction of a minutia as the reference direction. Once an ideal invariant value is mined, the same minutia produces the similar invariant values even if fingerprint images are changed. [11] In this condition, the technique does not damage the system performance because the relationships among the original fingerprint pattern are sealed in the transformed fingerprint pattern.

Ang et. al [12] presented a key-dependent transformation technique for producing cancelable fingerprint templates from fingerprint minutiae points. This technique creates templates by finding its core point initially, and a line through the core point is specified. The direction of the line is mentioned and calculated in the range of 0^o and 180^o by using the key transformation function. By altering the orientation, various templates are produced .However; it is impractical to find the correct location of core point.

2. Cryptographic key generation from multiple fingerprints and palmprint biometric

In the proposed approach, multiple fingerprints and palm print are selected as the biometrics for constructing cryptographic key. Minutiae points from the multiple fingerprints and from the palm print are mined which can be used for construct the cryptographic key. Figure 1 .represent Multiple Fingerprints Image. Figure 2 represent Palmprint Image. Figure 3 represent Step of Generating Cryptography key from Multiple Fingerprints. Figure 4 represent Generating Cryptography Key from Palmprint image.

Figure 1. Multiple Fingerprints Image

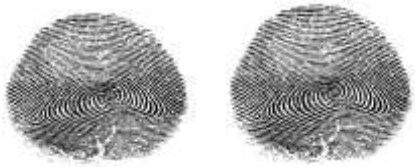
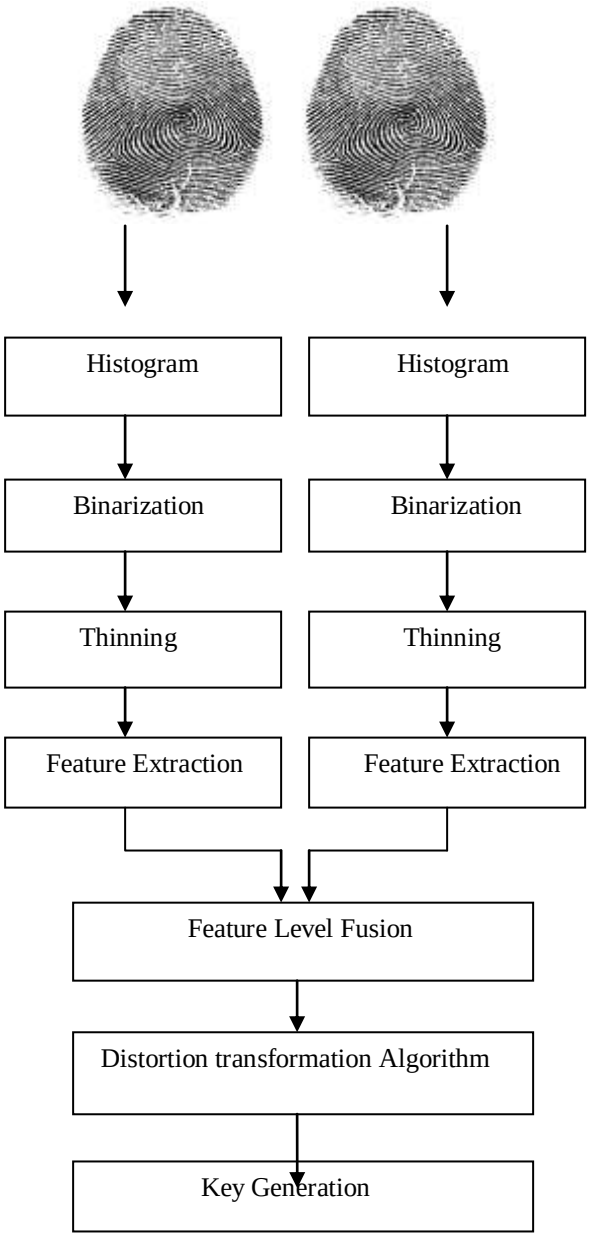


Figure 2. Palmprint Image

Figure 3. Steps for Generating Cryptography key from Multiple Fingerprints



2.1 Histogram Equalization

To expand the pixel value distribution of image the histogram equalization is used, that also used for increase the perceptional information. This is a method for adjust image intensities to improve the contrast. The given image is f that can be represented by matrix of integer pixel intensities ranging from 0 to L − 1.The number of possible intensity values is L, often 256. Let p represent the normalized histogram of f with a bin for every possible intensity.

So,

$$P_n = \frac{number\ \ of\ pixels\ \ with\ intensity\ \ n}{total\ \ number\ \ of\ pixels} \longrightarrow [1]$$

The histogram equalized image g will be defined by

$$g_{i,j} = \text{floor}(\ (L-1)\sum_{n=0}^{f_{i,j}} p_n) \longrightarrow [2]$$

The histogram of palm print and finger print is a unimodel type, after the histogram equalization process. Figure 5(a) represents Fingerprint Image before and after Histogram. Figure 5(b) represent Palmprint Image before and after Histogram .

Figure 4. Steps for Generating Cryptography Key from Palmprint image

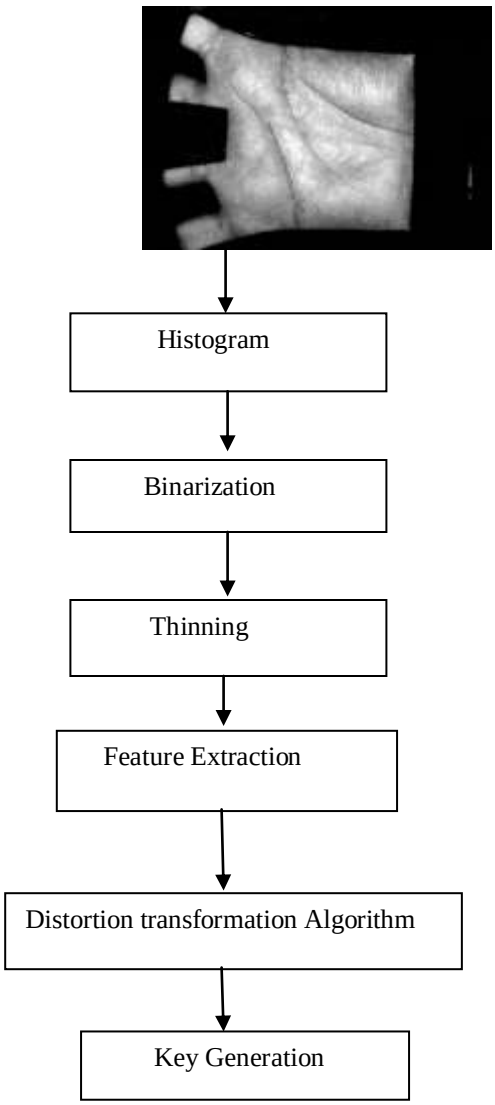


Figure 5(a) Fingerprint Image before and after Histogram

Figure 5(b) Palmprint Image before and after Histogram

Before After

2.2 Binarization

The conversion of grey level image into a binary image process is done by using binarization**.** Using this process, the contrast among ridges and valleys in a fingerprints and palmprint image are increased. Therefore, it is probable to mine the minutiae features. Consequently Binarization technique is involved to analyze grey level values of each and every pixel, if values is superior than the global threshold set binary value as 1 else 0.

The Binarization equalization is applied for in order to increase the contrast of the image.

$$c(i,j) = I_{\max}(i,j) - I_{min}(i,j) \longrightarrow [2]$$

where C(i, j) denotes the contrast of an image pixel (i, j), $I_{max}(i,j)$ and $I_{\min}(i,j)$denote the maximum and minimum intensities within a local neighborhood windows of (i, j).

The perceptional information of the image is improved by utilizing the binarization equalization process. It facilitates the pixel value to expand. The visualization of the fingerprint and palmprint image is represented in figure 6a and figure 6b.

Figure 6(a) Fingerprints before and after Binarization

Before After

Figure 6(b) Palmprint Image before and after Binarization

Before After

2.3 Thinning

The most important morphological method is thinning which is used to eliminate chosen foreground pixels from binary images. Thinning process is used in several applications such as Skeletonization. In this mode it is generally used to order the output of edge detectors by decreasing all lines to single pixel thickness. After the completion of thinning process it generates the binary image as output. The probability of an incidence of a pixel level *i* in the image is

$$P_x(i) = p(x = i) = \frac{n_i}{n}, 0 \leq i < L \text{.....[4]}$$

The total amount of gray levels in the image is *L*, the total amount of pixels in the image is *n*.

$$\mathrm{cdf_x(i)} = \sum_{j=0}^{i} \mathrm{p_x(j)} \longrightarrow [5]$$

$\mathrm{p_x(i)}$Being in fact the image's Thinning for pixel value i, regularized to [0,1]. Figure 7 represents Finger print and palmprint image after Thinning process.

Figure 7. Fingerprint and palmprint image after Thinning process

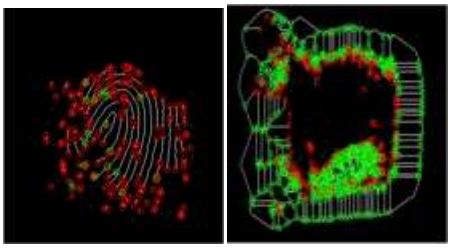
Fingerprint Palmprint

2.4 Feature extraction

The enhanced fingerprint image is then used for the minutiae point extraction. To perform the extraction operation, the Binarization and morphological actions are used to enhance fingerprint image. The grey level image is converted to binary image by using binarization method. The unwanted spurs and line breaks are removed by using Morphological process.

The unnecessary pixels are removed by using ridge thinning algorithm technique till the edge develops into one pixel wide. This thinning algorithm used for minutiae points mining in the proposed technique has been employed by the authors of [13]. From the thinned fingerprint image minutiae points are take out. The ridge ending and bifurcation are most important minutia features of fingerprint ridges.
Figure 8 represents Extracted features from Fingerprint and palm print image.

Figure 8. Extracted features from Fingerprint and palm print image



Fingerprint **Palmprint**

2.5 Feature Level Fusion for Multiple Fingerprints

The final step is generation of the k-bit cryptographic key from multiple biometric template T_B. The template vectorT_B is denoted as,

$$T_B = [t_1 t_2 t_3 \cdots t_d] \longrightarrow [6]$$

The vector T_B is then normalized to k components appropriate for generating the k-bit key. The normalization employed in the proposed approach is given as,

$$\mathrm{N} = \begin{cases} [t_1 t_2 \cdots t_k] \\ [t_1 t_2 \cdots t_d] \end{cases} \ll t_i; \mathrm{d} + 1 \geq \mathrm{i} \geq \mathrm{k} \longrightarrow [7]$$

Where, $t_i = \frac{1}{d} \sum_{j=1}^{d} t_j$

Finally, the key K_B is generated from the vector *N,*

$$K_B \ll \begin{cases} 1 \text{ if } N_i \geq N_{avg} \\ 0 \text{ if } N_i < N_{avg} \end{cases} ; i=1,2,3\ldots,k \longrightarrow [8]$$

Where, $N_{avg} = \frac{1}{k} \sum_{i=1}^{k} N_i$

It has been empirically selected as 6 pixels. The systems achieve 144 separate blocks of each and every fingerprint image. N square block pixels, i.e. *f(x, y)* are obtained.

2.6 Cryptographic Key Generation using Distortion algorithm

Enrollment: The system transforms original palm print data using the parameters provided by the user, and then stores the distortion form in the server database [14].

Recognition: The system transforms a sample of the user's palm print using parameters provided by the user, and then performs matching with the templates in the transformed form.

The proposed system stores only its noninvertible dissimilar version (e.g., a hash) as a replacement for storing the original biometrics data in the data base during employment. During identification, the proposed system would transform the data using the same noninvertible transform and carry out matching in the transformed space. Different applications can use various noninvertible distorted versions. The user can select the transform factor in terms of a password or PIN. If such a biometric template is cooperated, the system can create a novel one using a different transform or various parameters.

Let the minutiae Z (i) denoted as (x, y, α) in the Cartesian coordinate structure in whereas (x, y) represent the position of the minutiae and α represent the orientation point. Assume that R (Z_0) be the region and Z_0 represents the centered minutia. Consider that R (Z_0) have k minutiae then R (Z_0) is denoted as {Z_0,Z_1,…….Z_{k-1}}.

The steps to obtain the secured template are as follows:

1. Convert all minutiae of regions R(Z_0) from Cartesian to polar form
2. Rotate all minutiae of R(Z_0)at one time to guarantee the orientation of Z_0equals 90 and obtain the converted minutiae as (ρ,e_r, α_r)
3. Hash all minutiae in region R(Z_0)
   Consider the transform parameter a1, a2, b1, b2, c1, c2 a given by the user and hash values of minutiae are v1 and v2

$$V1 = a1^* \rho + b1^* e_r + c1^* \alpha_r \longrightarrow [9]$$
$$V2 = a2^* \rho + b2^* e_r + c2^* \alpha_r \longrightarrow [10]$$

4. Set of images of hashed minutia are returns as resultant.
5. Store the hashed region of image as a distortedly transformed Key in the database.

3. Results and discussions

This section discusses the results obtained for cryptographic key generation from palmprint as unimodal and two fingerprints of a same person is used for multiple biometric. The proposed system has been executed using MATLAB R2010a. The fingerprint and palmprint images are collected from FVC 2000 DB2, DB4-a database. The resolution of DB2 is 512 dpi and DB4-a is 500 dpi. The database consists of 800 fingerprint images and 600 palmprint images i.e., there are 200 persons, and each individual has four fingerprints and two palm prints.

The proposed system can be experimentally evaluated by using performance measures such as false rejection rate (FRR), false acceptance rate (FAR) and Accuracy.

False Rejection Rate (FRR)

FRR take place when a biometric system rejects a genuine user and wrongly labels that user as an intruder.

$$FRR(n) = \frac{\text{No of rejected verification attempts for a qualified person n}}{\text{No of all verification attempts for a qualified person n}} \quad [11]$$

False Acceptance Rate (FAR)

The FAR is the determination of the possibility that the biometric security system will wrongly accept an access attempt by an illegal user. A system's FAR naturally is stated as the ratio of the number of false acceptances divided by the number of identification attempts.

$$FAR(n) = \frac{\text{No of successful independent fraud attempts against a person n}}{\text{No of all independent fraud attempts against a person n}} \quad [12]$$

The following comparative Table 1 shows the experimental values obtained for Distorting transformation with multiple fingerprints and palm print of the same person. The proposed distortion transform is a method of transforming fingerprints and palm print, minutiae distortedly and achieving fingerprint and palm print, matching in the transformed space.

Table 1 Represents Performance analysis of distortion transformation

Cancelable distortion transformation performances are done on multiple fingerprints of a same person and palmprint images. The Table 1 shows the performances between both fingerprints and palmprint image. The FRR, FAR and accuracy value is calculated for both images and shown in this table.

Figure 9 represents Performance of Distortion Transformation with multiple fingerprints and palm print of the same person.

Figure 9.Performance of Distortion Transformation with multiple fingerprints and palm print of the same person

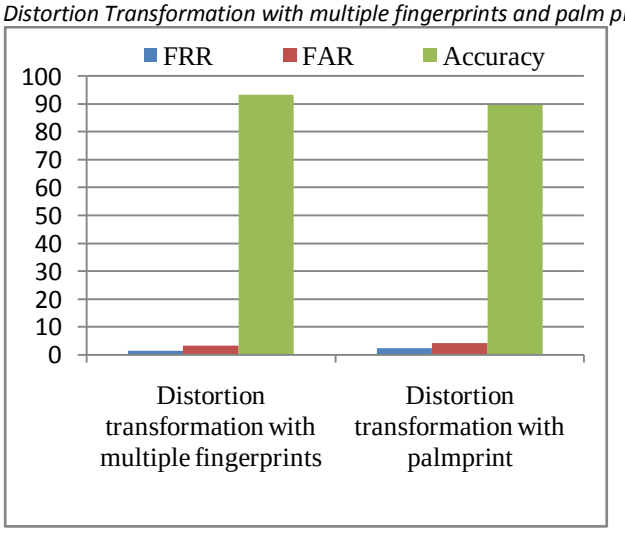


Table 1. Performance analysis of distortion transformation

Techniques	FRR %	FAR %	Accuracy %
Distortion with multiple fingerprints	1.4	3.3	93.31
Distortion with palmprint	2.3	4.2	89.73

The figure 9 shows the presentation of visual aid of distortion transformation. The performance is determined with multiple fingerprints and palmprint images of the same person. Cancellable biometric transformation algorithm that are used to generate cryptographic keys. Table 1 shows the performance measure of distortion transformation with multiple fingerprints and palmprint. Based on the obtained values the above graph can be plotted. From the above graph, it can be completed that the proposed work cancellable distortion transformation on improved.

4. Conclusion

Biometric system offers a lot of benefits over traditional based techniques. However, unimodal biometric possesses disadvantages as well. If the biometrics feature is stolen, it cannot be replaced for further security. Also, the damaged biometrics leads to wrong verification. To overcome this difficulty, the proposed work focuses on using palm print (it consists wide range of region) as unimodal features and two fingerprint of a same person is used for multiple biometric. While comparing to the existing methods, multiple biometric system offers several advantages. The cryptographic key generation of multiple finger print and palm print of the same person. Simulation results show that the multiple finger print has less FRR and FAR than the palmprint. For future work, Multimodal biometric can be used to improve the user verification and also different levels of fusion can be applied.

5. Reference

[1] N. K. Ratha, J. H. Connell, and R. M. Bolle [2009] Enhancing security and privacy in biometrics-based authentication systems, *IBM System*, Vol. 40, (3), pp. 614–634.

[2] M. D. Marsico, M. Nappi, and G. Tortora [2011] NABS: Novel approaches for biometric systems, *IEEE Transaction on pattern Analysis and Machine Intelligence*, Vol. 41, (4), pp. 481–493.

[3] V. Conti, C. Militello, F. Sorbello, and S. Vitabile [2010] A frequency-based approach for features fusion in fingerprint and iris multimodal biometric identification systems, *IEEE Transactions on System man and cybernetics part b applications and reviews.,* Vol. 40, (4), pp. 384–395.

[4] X. Jing, Y. Yao, D. Zhang, J. Yang, and M. Li. [2007] Face and palm print pixel level fusion and Kernel DCV-RBF classifier for small sample biometric recognition, *Pattern Recognition*, Vol. 40, (11), pp.3209-3224.

[5] W. Juang, S. Chen, and H. Liaw [2008] Robust and efficient password authenticated key agreement using smart cards, *IEEE Transactions on industrial electronics.,* Vol. 15, (6), pp.2551–2556.

[6] L. Hong, Y. Wang, and A. K. Jain [2009] Fingerprint image enhancement: Algorithm and performance evaluation, *IEEE Transactions on Pattern Analysis and Machine Intelligence.,* Vol. 21, (4), pp. 777–789.

[7] X. Li,W. Qiu, D. Zheng, K. Chen, and J. Li [2010] Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards, *IEEE Transactions on pattern Analysis and Machine Intelligence.*, Vol. 57, (2), pp. 793–800.

[8] L. Hong, Y. Wang, and A. K. Jain [2006] Fingerprint image enhancement: Algorithm and performance evaluation, *IEEE Transaction on Pattern Analysis and Machine Intelligence.,* Vol. 21, no. 4, pp. 777–789.

[9] R. Cappelli, M. Ferrara, and D. Maio [2012] A Fast and Accurate Palm print Recognition System Based on Minutiae, *IEEE Transaction on System, Man and Cybernetics Part b applications and reviews.,* Vol. 42, (3), pp. 1083-4419.

[10] C. Lee, J. Y. Choi, K. A. Toh, S. Lee, and J. Kim [2007] Alignment-free cancellable fingerprint templates based on local minutiae information, *IEEE Transactions on system man and cybernetics part c applications and reviews.,* vol 37, (4), pp. 980–992.

[11] K. Nandakumar, A. K. Jain, and S. Pankanti [2007] Fingerprint-based fuzzy vault: Implementation and performance, *IEEE Transactions on information forensics and security,* Vol. 2, (4), pp. 744–757.

[12] Ross and A. Othman [2011] Visual cryptography for biometric privacy*, IEEE Transactions on information forensics and security,* Vol. 6, (1), pp. 70–81.

[13] J. Dai, J. Feng and J. Zhou [2009] Robust and Efficient Ridge-Based Palm print Matching, *IEEE Transaction on Pattern Analysis and Machine Intelligence*, Vol.34, (8), pp. 0162-8828.

[14] J. You, W. Kong, D. Zhang, and K. Cheung [2010] On hierarchical palm print coding with multiple features for personal identification in large databases, *IEEE Transactions circuits systems video technology*, Vol. 14, (2), pp. 234–243.

The Publication fee is defrayed by Indian Society for Education and Environment (iSee). www.iseeadyar.org

Citation:

N.Gomathy and Dr.N.Radha [2014] Performance Analysis of Cancelable Unimodal and Multiple Biometric Using Distortion Transformation Algorithm . *Indian Journal of Innovations and Developments.* Vol 3 (3), pp. 50-60.