Survey On Robust Security Using Code Level Approach For Iris Recognition

Ms.C.Nigila [1], (Professor)Mrs.G.Gandhimathi [2]
[1, 2] Dept of ECE
[1, 2] Parisutham Institute of Technology & Science,
Thanjavur.

Abstract- *It is a security based concept in the fields where we are using our iris. The proposed concept holds two techniques. Using code level approaches to find the iris features in a human eye is the initial step followed by weight mask for iris features in both eyes and analysis the same matching given only by the person. In MATLAB the approach mainly involves extraction of features from the sample fingerprint images and then performing iris matching based on the number of features among iris images. Thus no one can access the data of a person whose system holds this security system as that particular person only knows the correct order of the iris for authentication purpose.*

Keywords- iris features.

I. INTRODUCTION

In MATLAB the approach mainly involves extraction of features from the sample fingerprint images and then performing iris matching based on the number of features among iris images. Thus no one can access the data of a person whose system holds this security system as that particular person only knows the correct order of the iris for authentication purpose.

II. LITERATURE SURVEY

Matching heterogeneous iris images in less constrained applications of iris biometrics is becoming a challenging task. The existing solutions try to reduce the difference between heterogeneous iris images in pixel intensities or filtered features. In contrast, this paper proposes a code-level approach in heterogeneous iris recognition. The non-linear relationship between binary feature codes of heterogeneous iris images is modeled by an adapted Markov network. This model transforms the number of iris templates in the probe into a homogenous iris template corresponding to the gallery sample. In addition, a weight map on the reliability of binary codes in the iris template can be derived from the model. The learnt iris template and weight map are jointly used in building a robust iris matcher against the variations of imaging sensors, capturing distance and subject conditions. Extensive experimental results of matching cross sensor, high-resolution vs low-resolution and, clear vs blurred iris images demonstrate the code-level approach can achieve the highest accuracy in compared to the existing pixel level, feature level and score-level solutions.

RIS biometrics provides a reliable method for personal identification in most mission-critical applications. Great advancement in iris recognition can achieve extremely high accuracy of identity verification with uniform iris sensors, close imaging distance, and cooperative users. The probe and gallery iris images captured in controlled conditions are of high quality and they facilitate effective matching. However, other applications are needed to extend iris recognition to less constrained scenarios. For example, iris at a distance and iris on the move systems have been developed for surveillance applications. Similarly, iris recognition modules are integrated into mobile devices. It is possible to use different types of iris sensors to build a large scale or wide-area identity management system such as the Unique Identification Authority of India project. [1].

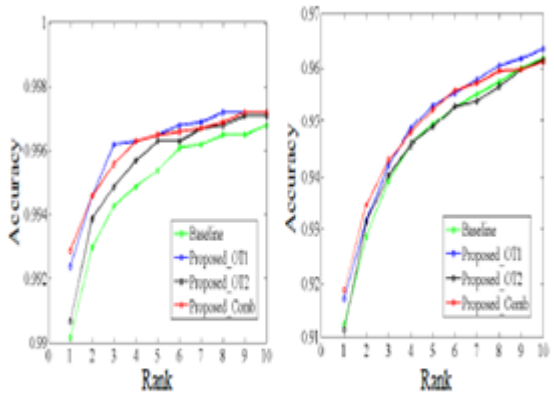
The calculation of binary iris codes from feature values (e.g. the result of Gabor transform) is a key step iniris recognition systems. Traditional binarization method basedon the sign of feature values has achieved very promisingperformance. However, currently, little research focuses on adeeper insight into this binarization method to produce iriscodes. In this paper, we illustrate the iris code calculationfrom the perspective of optimization. We demonstrate that thetraditional iris code is the solution of an optimization problemwhich minimizes the distance between the feature values and iriscodes. Furthermore, we show that more effective iris codes canbe obtained by adding terms to the objective function of thisoptimization problem. We investigate two additional objectiveterms. The first objective term exploits the spatial relationships ofthe bits in different positions of an iris code. The second objectiveterm mitigates the influence of less reliable bits in iris codes. Thetwo objective terms can be applied to the optimization problemindividually, or in a combined scheme. We conduct experimentson four benchmark datasets with varying image quality. Theexperimental results demonstrate that the iris code producedby solving the optimization problem with the two

additionalobjective terms achieves a generally improved performance incomparison to the traditional iris code calculated by binarizingfeature values based on their signs. The advancement of game technologies have now made itpossible to create realistic, highly interactive environments at an affordable and relatively quick production time. This paper investigates into the use of game engines to develop a highly interactive virtual campus tour application. There is a discussion into the approach taken and the challenges faced with this solution to the navigation and exploration of interior of buildings. Section II describes the common virtual campus tour solutions that are currently in use by most of the UK Universities[2].

HE iris has become one of the most reliable biometric traits for human authentication due to some inherentadvantages, for example, it is a highly protected internal organwhich is visible externally; iris patterns are highly distinctivewith a high degree of freedom; iris patterns are relatively stable over time etc. State-of-the-art iris recognition algorithmshave reported promising performance. Most of thesealgorithms use binary features (i.e. iris codes). The binarynature of iris codes brings significant advantage in memoryand computational cost, enabling the large scale deploymentof iris recognition systems. Current nationwide deployments ofiris recognition systems in UAE and India are considered successful, with millions of subjects enrolled. Alternativefeature extraction and selection approach instead of binary iriscodes have also shown high effectiveness.

A traditional iris recognition system mainly consists of three components: iris segmentation, feature extraction andiris matching.

Our contribution is as follows. First, Weinvestigate the iris code production from the perspective of optimization. We demonstrate that traditional iris codes basedon the sign of feature values are the solution of an optimization problem. Second, based on this optimization problem, we propose two additional objective terms to obtain more effective iris codes. The first objective term exploits the spatial relationship of the bits in different positions of an iris code, while the second objective term mitigates the influence of less reliable bits in iris codes. Experimentally, we find that the two objective terms are able to improve the incorrect iris matching result when using the traditional iris code caused by factors such as the imaging variation in different captures. Third, we



(a) CMC, CASIAT (b) CMC, ND0405

propose a scheme to combine the two additional objectiveterms. We show that the iris code obtained by the combinedscheme achieves a generally improved performance, comparedto traditional iris codes and the iris codes obtained using eachindividual objective term.

The remainder of this paper is organized as follows we present the proposed method to produce iriscodes based on optimization. the result of experimental analysis of the proposed method. Finally in, we concluded the paper. [3].

Iris Recognition is one of the important biometric recognition systems that identify people based on their eyes and iris. In this paper the iris recognition algorithm is implemented via histogram equalization andwavelet techniques. In this paper the iris recognition approach is implemented via many steps, these steps are concentrated on image capturing, enhancement and identification. Different types of edge detection Mechanisms; Canny scheme, Prewitt scheme, Roberts scheme and Sobel scheme are used to detect iris boundaries in the eyes digital image. The implemented system gives adequate results via different types of iris images.

Electronic arena is witnessing rapid sophisticated, a large and important. Recognition systems have become a role of the large and effective, especially after the progress that has occurred inthe area of Information Technology. Iris is the main important part of the human eye; it consistsof circular muscle and the other longitudinal control in the amount of light passing the retinathrough the human eye, with the increasing of requirements for higher security level, biometricsystems have been widely used for many applications. Biometrics includes face, iris, fingerprints,voice, palms, hand geometry, retina, handwriting, gait etc.

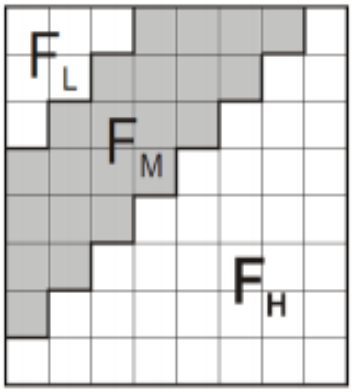
A biometric system is fundamentally a pattern-recognition system that recognizes a individual based on a attribute vector derived from a specific physiological or behavioral characteristic thatthe person possesses. That feature vector is frequently stored in a database (or recorded on asmart card given to the individual) after being extracted. A biometric system based onphysiological characteristics is normally more reliable than one which adopts behavioralcharacteristics, even if the last may be easier to integrate within certain specific application.Biometric system can than run in two modes: verification or identification. While recognitioninvolves comparing the acquired biometric information against templates corresponding to allusers in the database, verification involves comparison with only those templates correspondingto the claimed identity. This implies that identification and verification are two problems thatshould be dealt with separately.

A simple biometric system consists of four basic components

- Sensor module witch acquires the biometric data.
- Feature extraction module where the acquire data is processed to extract feature vectors.
- Matching module where attribute vectors are compared against those in the template.
- Decision-making module in which the user's identity is established or a claimed identity is accepted or rejected. [3].

This paper presents novel security architecturefor protecting the integrity of iris images and templates usingwatermarking and Visual Cryptography (VC). The proposedscheme offers a complete protection framework for the iris biometrics which consists of two stages: the first stage is for irisimage protection while the second is for the iris template. Firstly,for protecting the iris image, a watermark text which carries personal information is embedded in the middle band frequencyregion of the iris image using a novel watermarking algorithmthat randomly interchanges multiple middle band pairs of theDiscrete Cosine Transform (DCT). Secondly, for iris templateprotection, the binary iris template is divided into two sharesusing VC, where one share is stored in the database and theother is kept with the user on a smart card. In addition, theSHA-2 hash function is utilized to maintain the integrity of the stored iris template in both the database and smart card.The experimental and comparison results on the CASIA V4and UBIRIS V1 iris databases demonstrate that the proposed framework preserves the privacy of the iris images and templatesand retains robustness to malicious attacks while it does not havea discernible effect on the recognition performance.

The fact that biometric systems offer reliabletechniques for personal identification, their usage could be hampered by the lack of a proper protection scheme that guarantees the security and privacy of the biometric traits. When biometric images or templates are transmitted through insecure channels or stored as raw data, they run risks of being stolen or modified. Hence, it is imperative that robust and reliable means of biometric protection are implemented. Rathaet describedeight types of attacks that are possible in a biometric system, such as database template tampering, template modification, the matcher override of the final decision and attack on the channel between the feature extractor and the matcher, or attack on the channel between the database and matcher. Moreover, due to the wide spread of biometrics technology in many applications, it is very likely that biometric data are being transmitted over non secure channels.[4].



Frequency regions in an 8 × 8 DCT block

Iris recognition systems are increasingly deployedfor large-scale applications such as national ID programs whichcontinue to acquire millions of iris images to establish identityamong billions. However with the availability of variety of irissensors that are deployed for the iris imaging under differentillumination/environment, significant performance degradation isexpected while matching such iris images acquired under twodifferent domains (either sensor-specific or wavelength-specific).

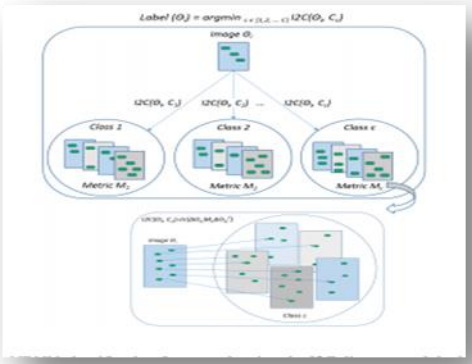
This paper develops a domain adaptation framework to address this problem and introduces a new algorithm using Markovrandom fields (MRF) model to significantly improve cross-domainiris recognition. The proposed domain adaptation frameworkbased on the naive Bayes nearest neighbor classification usesa real-valued feature representation which is capable of learning domain knowledge. Our approach to estimate correspondingvisible iris patterns from the synthesis of iris patches in the nearinfrared iris images achieves outperforming results for the cross-spectral iris recognition. In

this paper, a new class of bi-spectraliris recognition system that can simultaneously acquire visibleand near infra-red images with pixel-to-pixel correspondences isproposed and evaluated. We present reproducible experimentalresults from three publicly available databases; PolyU cross-spectral iris image database, IIITD CLI and UND database,and achieve outperforming results for the cross-sensor and cross-spectral iris matching.

RIS recognition plays an important role in uniquely identifying a person and is based on the uniqueness ofiris texture. As compared to several other biometrics, irisrecognition system is believed to be more reliable, accurate and scalable for person identification. Therefore the irisrecognition system is widely used in large-scale national IDprograms (e.g., IndiasAadhaar and UAEs border securityprograms) for processing over millions/billions of peoplesbiometric data. However several challenges emerge when theiris images acquired in one domain (sensor or illumination) ismatched against the images acquired in different domain. Suchcross-domain iris recognition problem includes the cases whenthe images in one domain represent the sensor-specific irisimages or wavelength-specific iris images.

This cross-domainiris recognition problem is briefly discussed in two differentcontexts of iris cross-comparisons.NBNN classification framework using the I2C distance and the learned Per-Class metric (Mahalanobis distance). The large variations in iris similarity scores from the cross-domain iris matching can be attributed to the mismatch ofimaging wavelengths,

Circles and rectangles represent theclass labels and images, respectively. Local feature descriptors are illustrated as green colored points [5].



In today's world security is becoming more and more important. Authentication plays a major role in security.Authentication is the process of verifying the claimed identityof a person. Authentication is a means of defence againstintruders. There are of various types like authentication usingusername with password, using card and using biometric. Most commonly, username with password is used for authentication, but Password is easily carked or stolen becauseof human tendency to make password easy to remember andalso note down the password so that there is no need toremember. Cards can be stolen and accessing by anyone.Therefore there is no way of knowing that the claimed personis the actual one. Biometric identification provides secureauthentication of a person as biometric data can't be steal andduplicated. Biometric data is unique and permanentlyassociated with a person.

Iris recognition is a method of biometric identification. Biometric identification provides automatic recognition of anindividual based on the unique feature of physiologicalcharacteristics like fingerprints, DNA, palm, face, iris, veinand retina or behavioural characteristic like Handwriting,speech and signature.

Iris recognition is a method of recognizing a person by analysing the iris pattern. Iris pattern are formed by six monthsafter birth. Iris pattern remains stable after a year and remainthe same for life time that means it does not have aging effect.Iris patterns of identical twins differ and a person's left andright eyes have different patterns as well. This distinguishes itfrom fingerprints or palm print, which can be difficult torecognize after years of certain types of manual labor. It isregarded as the most reliable biometric technology since iris ishighly distinctive and robust.

Iris recognition consists of five basic modules:

- Image Acquisition: Obtains an image of the eye.
- Iris Segmentation: Localizes the iris's spatial extentby isolating it from other structures in its vicinity,such as the sclera, pupil, eyelids, aneyelashes.
- Normalization: A geometric normalization scheme totransform the segmented iris image from Cartesiancoordinates to polar coordinates.
- Feature Extraction: The most discriminating informationpresent in an iris pattern mus be extracted.

Matching: determines how closely the produced codematches the encoded features stored in the database.. [6].

(VR) will be a profoundly disruptive technology in the same way as the Smartphoneand the Internet. Like the Smartphone, VR uses anew interface format (a head-mounted

display andhand controllers) to provide much more intuitive andnatural access to a computing device. Much like the Internet, itallows a new kind of worldwide communication but thistime with a natural human experience that will be nearly indistinguishable from standing face to face or in a group.

Thecombination of these two capabilities, along with a price pointsimilar to the first smart phones, suggests that we will see anadoption curve similar to that of the Smartphone, with a majority of worldwide Internet users making daily use of VR in thenext seven to ten years.

VR technology has been demonstrated multiple times inprior years, in ways that were nearly as compelling as thecurrently available Oculus Rift, HTC Vive, and SamsungGearVR devices.

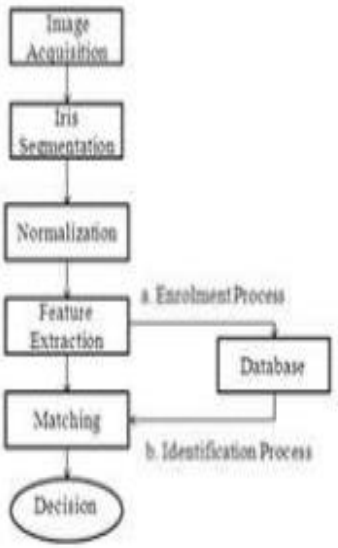
The big difference this time has been drivenby the intense competition in the Smartphone market toreduce the size and cost of orientation sensors and high-resolution displays to finally make these research devices available for consumers.

The same advances have madelightweight wireless handheld controllers that track themotion of the hands and/or fingers with very high accuracypossible. Another factor that has changed is Internet speedand latency.

One-way Internet transmission times, even half-way around the world, are now short enough to allow twopeople to talk face to face as digital avatars without beingable to detect the delay, making communication completely natural.

Iris recognition is a method of biometric identification.Biometric identification provides automatic recognition of anindividual based on the unique feature of physiologicalcharacteristics or behavioural characteristic. Iris recognition is amethod of recognizing a person by analysing the iris pattern.This survey paper covers the different iris recognition techniquesand methods.

This level of interaction had to wait forInternet speeds and routers to reach their current levels ofperformance, which are now close to the limits set by thespeed of light. [7].



Due to security countermeasure Iriscomparison and recognition has better precision as compare to the other biometrics features such as face recognition, finger prints, palm veins, face recognition, DNA, palm print, hand geometry etc. Many algorithms are used to increase the iris comparison and recognition performance. This paper shows the different steps which are used to verify the Iris comparison and recognition performance between the template image and query image. We created a code in MATLAB software which allows the assimilation of iris which gives the erudition about the iris images. It focuses on the recognizing the identity of an individual and shows the characteristics pattern of the iris.

Here it is also shows that template and query image is same then the result is identical. Otherwise they are non-identical. This simulation result is obtained by using MATLAB which is effective as well as reliable and it is used as security purpose and to manage the level of stress.Biometrics authentication process is a form of identification and access control. It identifies an individual in groups that are under surveillance. Authentication process is a technique which is used to verify an identity affirmed for a system or person. The information which is recycled for identifying and verifying the user is depend on the information which is known by authenticated user, such as personal question, password and personal identification number. But the above authentication methods are cost effective and can be suffers several security attacks such as eavesdropping, guessing etc.

In biometrics authentication can be done by severalprocess such as fingerprint, voice key stock pattern, retinal pattern, hand geometry, and iris. These authentications have some advantages because inthese users have not remember anything like PIN code, password etc. But in

several biometric authentications may require their unadoptable cost.

Among all the authentication system iris comparisonand recognition system which is used to find that the people with identical and non-identical pattern. Therefore iris comparison and recognition is best solution for people identification as network access. Compare to the other authentication process iris is protected from the external province . Nowadays,a various types of iris recognition system have been proposed, in which it has found that they uses multiple resolution techniques with the help of the recognition algorithm which provide a representation.

In 1993 Shapiro provide a multi-resolution technique that is based on Embedded Zerotree Wavelet (EZW).Chou et al. proposed an iris comparison and recognition system which consists of non-orthogonal observation of dual charge coupled device camera which is helped to capture the four spectral iris images. The iris texture needs various distinctive information which are used for the personal recognition.

The iris pattern varies person to person which is obtained through video based system. It has a complex pattern and it is a combination of different characteristics known as pits, furrows, freckles, corona, striation and rings. The iris authentication is non-invasive secured can be used for taking care of administration. Iris comparison and recognition can be an approved to access the mobile phone workstations, machine system and ATM. It is a best method in field of security and it raises the interest in unsharp masking techniques. PSNR and MSE are two basic technique toanalyze and explore Iris based human identification using MATLAB are presented. Here Section II and section III describes different iris recognition technique used and also describes about simulation results respectively. Using MATLAB software various technique are analyse and finally iris recognition system are used in various applications such as security purpose, managing of stress in home by using the authenticated person who can only enter the house by these technique [8].

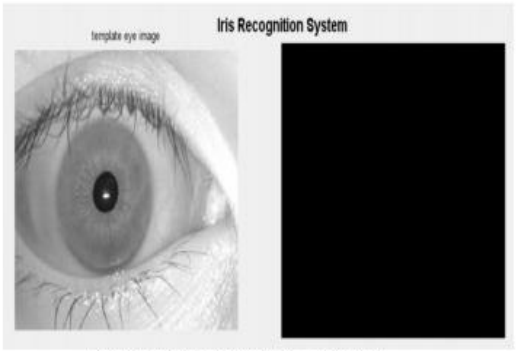


Fig 2: Loading of template eye image.

III. CONSLUCTION

In this paper are analysis of different type of iris realisation methods realityand the concept is to make an application for authentication of various security system usages

REFERENCES

[1] P. Stavroulakis and M. Stamp, Handbook of Information and Communication Security.Springer, 2010.

[2] N. Ratha, J. Connell, and R. Bolle, An Analysis of Minutiae Matching Strength. Springer Berlin Heidelberg, 2001, vol. 2091, book section 32, pp. 223–228.

[3] K. Martin, L. Haiping, F. M. Bui, K. N. Plataniotis, and D. Hatzinakos, "A biometric encryption system for the self-exclusion scenario of face recognition," IEEE Systems Journal, vol. 3, no. 4, pp. 440–450, 2009.

[4] A. Jain, A. Ross, and U. Uludag, "Biometric template security: Challenges and solutions," in 13th European Signal Processing Conference, EUSIPCO05, 2005, pp. 1–4.

[5] J. Daugman, "How iris recognition works," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 21–30, 2004.

[6] S. Venugopalan and M. Savvides, "How to generate spoofed irises froman iris code template," IEEE Transactions on Information Forensics and Security, vol. 6, no. 2, pp. 385–395, 2011.

[7] J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez, and J. Ortega- Garcia, "Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms," Computer Vision and Image Understanding, vol. 117, no. 10, pp. 1512–1525, 2013.

[8] K. Park, D. Jeong, B. Kang, and E. Lee, A Study on Iris Feature Watermarking on Face Data. Springer Berlin Heidelberg, 2007, vol. 4432, book section 47, pp. 415–423.

[9] A. Hassanien, A. Abraham, and C. Grosan, "Spiking neural network and wavelets for hiding iris data in digital images," Soft Computing, vol. 13, no. 4, pp. 401–416, 2009.

[10] S. Majumder, K. J. Devi, and S. K. Sarkar, "Singular value decomposition and wavelet-based iris biometric watermarking," IET Biometrics, vol. 2, no. 1, pp. 21–27, 2013.

[11] M. Paunwala and S. Patnaik, "Biometric template protection with DCT- based watermarking," Machine Vision and Applications, vol. 25, no. 1, pp. 263–275, 2014.

[12] M. A. M. Abdullah, S. S. Dlay, and W. L. Woo, "Securing irisimages with a robust watermarking algorithm based on Discrete Cosine Transform," in Proceedings of the 10th International Conference on Computer Vision Theory and Applications, vol. 3, 2015, pp. 108–114.

[13] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," IEEE Transactions on Computers, vol. 55, no. 9, pp.1081–1088, 2006.

[14] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zemor"Theoretical and practical boundaries of binary secure sketches," IEEE Transactions onInformation Forensics and Security, vol. 3, no. 4, pp. 673–683, 2008.

[15] S. Yan, Z. Xukai, E. Y. Du, and L. Feng, "Design and analysis of a highly user-friendly, secure, privacy-preserving, and revocable authentication method," IEEE Transactions on Computers, vol. 63, no. 4, pp. 902– 916, 2014.

[16] S. Cimato, M. Gamassi, V. Piuri, R.Sassi, and F. Scotti, A Multi- biometric Verification System for the Privacy Protection of Iris Tem- plates. Springer Berlin Heidelberg, 2009, vol. 53, book section 29, pp. 227–234.

[17] C. Rathgeb, F. Breitinger, C. Busch, and H. Baier, "On application of bloom filters to iris biometrics," IET Biometrics, vol. 3, no. 4, pp. 207–218, 2014.

[18] J. Hermans, B. Mennink, and R. Peeters, "When a bloom filter is a doom filter: Security assessment of a novel iris biometric template protection system," in International Conference of the Biometrics Special Interest Group (BIOSIG), 2014, pp. 1–6.

[19] D. Aeloor and A. Manjrekar, Securing Biometric Data with Visual Cryptography and Steganography. Springer Berlin Heidelberg, 2013, vol. 377, book section 33, pp. 330–340.

[20] K. Anusree and G. S. Binu, "Biometric privacy using visual cryptog- raphy, halftoning and watermarking for multiple secrets," in National Conference on Communication, Signal Processing and Networking, 2014, pp. 1–5.

[21] W. Yiwei, J. F. Doherty, and R. E. Van, "A wavelet-based watermarking algorithm for ownership verification of digital images," IEEE Transactions on Image Processing, vol. 11, no. 2, pp. 77–88, 2002.

[22] D. P. Mukherjee, S. Maitra, and S. T. Acton, "Spatial domain digital watermarking of multimedia objects for buyer authentication," IEEE Transactions on Multimedia, vol. 6, no. 1, pp. 1–15, 2004.

[23] R. G. Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in IEEE International Conference Image Processing, ICIP-94., vol. 2, 1994, pp. 86–90.

[24] R. M. Thanki, R. K. Kher, and D. Vyas, "Robustness of correlation based watermarking techniques using WGN against different order statistics filters," International Journal of Computer Science and Telecommunications, vol. 2, no. 4, pp. 45–49, 2011.

[25] P. Dabas and K. Khanna, "A study on spatial and transform domain watermarking techniques," International Journal of Computer Applications, vol. 71, no. 14, pp. 38–41, 2013.[26] Roger E Kirk. Experimental design.Wiley Online Library, 1982.