Review on various Face Artefact Detection mechanism

Prabhjot kaur[1], Rohit Mahajan[2]
[1,2] *Golden College of Engineering and Technology Gurdaspur, India*

***Abstract*- To automatically recognition of face is wide utilized in a few applications like confirmation of portable payment. Programmed face recognition has raised issues concerning face artefact detection (biometric sensor introduction assaults), in which a photo or video of an approved individual's face will be utilized to pick up access. There are assortments of face attack discovery strategies are proposed, their speculation capacity has not been sufficiently tended to. The goal of this paper is to review and recognize various face attack detection ways and to sort them into entirely unexpected classes.**

***Index terms*- DCT, Face Attack, Image Processing**

I.INTRODUCTION

Automatic face recognition has pulled in expanding consideration in a few get the opportunity to control applications, altogether for versatile opening. Like unique mark verification, with the arrival of face opening common sense inside the Android portable working framework bundle, face recognition transforms into another biometric recognizable proof procedure for versatile phones(Touch ID) inside the iOS framework. In no appreciation like unique mark verification, face recognition needn't bother with any further locator since each single propelled portable return furnished with a front end camera. Be that since it may, as various biometric modalities, we need to deal with stresses concerning face spoof ambushes on face recognition frameworks, especially in free police examination and uncooperative subject things[8].In resentment of the very truth that a paltry undertaking for the human mind, face recognition has swung to be enormously debilitating to mimic by counterfeit methods, since the shared characteristics do exist between faces, they contrast imposingly in wording age, skin, color and sexual orientation. The issue is extra wooly-disapproved by various picture characteristics, outward appearances, facial article of furniture, foundation and light conditions.

1.1 Image Processing

Image processing now days is used widely in order to transfer the data from source towards destination. It may contain additional information hidden by the user within the image. Transfer of images from networked medium may lead to the distortion due to presence of abnormalities. These abnormalities may be due to malicious attacks. These attacks on images that lead to distortion of images are known as attack. Attack within the image is a common attack that leads to misleading information. Thus, data at receiver end is not accurate leading to deception.

With the advancement in technology image processing tools and techniques are available for altering the images for attack. The modification or changes in current image is vital to detect since this image can be used in the authentication process. Image credibility hence required to be verified. This is accomplished by the use of attack detection mechanism. There are legion of ways by which image can be tempered. For example: re-sampling, copy and move, splicing etc.

Copy move is not new rather it is an exceptionally old issue. [3] Earlier this is restricted to writing only but with the advancement of technology, this copy move attack becomes critically part of images. Computerized software is used greatly for this imitation. Image can be easily changed and controlled by the use of computerised software. It is exceedingly difficult to identify any modification to the existing image.

[6]Image tempering causes loss of information that could be vital to the organization. Falsification is an issue and required to be tackled. For this purpose, attack detection mechanisms are provided. Procedures are required to be invented to detect the modification to the original image. Image attack detection is one of the essential issues associated with the forensic science.

The main objective of this paper is to present various image attack detection procedures; to review some

existing and new pixel based image attack detection mechanisms and to present comparative study of existing procedures used in image attack detection. Rest of the paper is organised as follows. Overview of image attack detection is presented in the first section, in second section image attack types are discussed, in third section image attack detection mechanisms are discussed and in forth section literature and comparison of various image attack detection mechanisms is presented. Last section gives the conclusion of this paper.

1.2 Types of attack in Images

Image attack involves addition of additional pixel or cutting some pixel intensity levels. Deleting some critical features is also objective associated with image attack. There are distinct methods which are used to forge a digital image. Taking into consideration all of those method, image attack is divided into following categories.

1) Copy Move attack
2) Image Retouching
3) Image Splicing
4) Image re-sampling

1.3 Copy Move Image attack

[13][4]Copy move attack mechanism is also known as cloning. Some part of the image is cut in any size and pasted on some other region in this case. Critical information either is lost or replicated in his case. As the copied part originated from the same image hence determining attack becomes very difficult.

Fig.|| Copy Move attack Example

1.4 Image Retouching

This is relatively less impactful attack mechanism in which image does not alter much. The image features are reduced or enhanced in this case. The contrast or colour of the image is changed but these types of defects are difficult to detect since image alteration is not up to great extents.

1.5 Segment Based attack

This is another rarely occurring attack mechanism within the image. Image is composed of large number of segments or blocks. All of these blocks are sequenced. In this type of attack, the sequenced blocks are changed to distort the image. Large portion of the image is distorted by the use of this attack. Segmentation mechanisms are required in ordered to tackle the problem.

1.6 Image attack using image Splicing

[4][10]Image splicing uses cut and paste method form one or more images to create a new image. The new image is also known as fake image. This is one of the most common types of attack mechanism. These mechanisms along with the copy move forged images are difficult to detect since image intensity levels does not differ much from the original image.

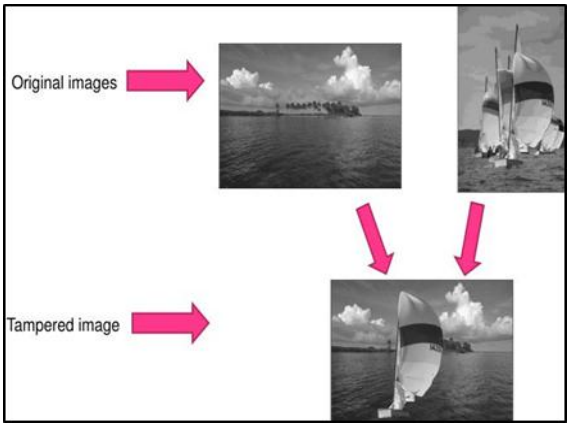

Fig.|| Image Splicing Example

1.7 Image Re-sampling

[14]This is another critical method of image attack. In this method some part of the image undergoes transformation. Transformation includes translation, rotation, scaling etc. The transformation used in this case could be uniform or non uniform. Uniform transformation does not alter the shape of the image. The non –uniform transformation on the other hand alter the shape of the image.

Fig.|| Image Re-Sampling Example

The primary focus of study is copy move and image splicing strategies for future enhancements.

Literature Survey

Image attack Detection Mechanisms are critical and are divided into following two categories:

Active and passive attack detection

Active attack detection mechanism is those in which additional information is packed along with the image for attack detection. Digital watermarking is an example of it. The problem with this approach is that space requirements associated with attack detection mechanism enhances greatly. In passive mechanism predefined information is not merged at capturing time and hence consumes much less space as compared to active attack detection mechanism. Binary patterns are analysed for attack detection in case of passive attack detection. Passive image attack detection is divided into following categories.

Pixel based Approach

[3]This approach analysis the pixels associated with the given image. Pixel composed of RGB intensity levels. These intensity levels are tempered with in case of attack. These pixel based approaches are divided into categories including copy move, splicing, re-sampling and statistical. We will focus on copy move and splicing techniques for image attack detection since they are most commonly used mechanism for attack detection. Under pixel based approaches following techniques appear.

PCA

[19]PCA indicates principal component analysis. This mechanism is used to extract the features associated with the image. The extracted features are selected using the priority analysis mechanism. The features having the priority above the threshold value are selected for examination. PCA reduces the complexity associated with image by reducing the feature analysis by selecting the necessary features only.

DCT

The Discrete Cosine Transform (DCT) calculation is outstanding and regularly utilized for picture pressure. DCT changes over the pixels in a picture, into sets of spatial frequencies. It has been picked in light of the fact that it is the best estimate of the Karhunen_loeve transform that gives the best pressure proportion. [26] The DCT work by isolating pictures into the parts of various frequencies. Amid a stage called Quantization, where parts of pressure really happen, the less vital frequencies are disposed of, henceforth the utilization of the lossy. At that point the most essential frequencies that remain are utilized recover the picture in deterioration process. Subsequently, remade picture is twisted Format Based Approach.

In the 1-D case the DCT is defined as

$$X_C(k) \triangleq \begin{cases} \sum_{n=0}^{N-1} 2x(n)\cos\frac{\pi k}{2N}(2n+1), & k \in [0, N-1] \\ 0, & else. \end{cases} \rightarrow (4)$$

for every N point signal $x(n)$ having support $[0, N-1]$. The corresponding inverse transform, or IDCT, can be written as

$$x(n) = \begin{cases} \frac{1}{N}\sum_{K=0}^{N-1} w(k)X_C(k)\cos\frac{\pi k}{2N}(2n+1), & n \in [0, N-1] \\ 0, & else. \end{cases} \rightarrow (5)$$

It turns out that this 1-D DCT can be understood in terms of the DFT of a symmetrically extended sequence,

$$y(n) \triangleq x(n) + x(2N-1-n) \rightarrow (6)$$

This is not the only way to symmetrically extend *x*, but this method results in the most widely used DCT sometimes calledDCT-2 with support $[0, 2N-1]$. In fact, on defining the 2N point DFT $Y(k) \triangleq DFT_{2N}\{y(n)\}$, we will show that the DCT can be alternatively expressed as

$$X_C(k) = \begin{cases} W_{2N}^{k/2} Y(k), & k \in [0, N-1] \\ 0, & else. \end{cases} \rightarrow (7)$$

Thus the DCT is just the DFT analysis of the symmetrically extended signal defined in (6):

Looking at this equation, we see that there is no overlap in its two components, which fit together without a gap. We can see that right after $x(N-1)$ comes $x(N-1)$ at position

$n = N$, which is then followed by the rest of the nonzero part of x in reverse order, upto $n = 2N - 1$, where sits $x(0)$ .We can see a point of symmetry midway between $n = N - 1$ and N, i.e., at $n = N - \frac{1}{2}$ If we consider its periodic extension $\tilde{y}(n),$ we will also see a symmetry about the point $n = -\frac{1}{2}$ We thus expect that the *2N* point $Y(k)$ will be real valued except for the phase factor $W_{2N}^{-k/2}$. So the phase factor in eqn (7) is just what is needed to cancel out the phase term in Y and make the DCT real , as it must if the two equations, (1) and (7), are to agree for real valued inputs *x*.

To reconcile these two definitions, we start out with eqn (7), and proceed as follows:

$$
\begin{aligned}
&Y(k) \\
&= \sum_{n=0}^{N-1} x(n) W_{2N}^{nk} + \sum_{n=N}^{2N-1} x(2N-1-n) W_{2N}^{nk} \\
&= \sum_{n=0}^{N-1} x(n) W_{2N}^{nk} + \sum_{n'=0}^{N-1} x(n') W_{2N}^{-(n'+1)k}, \ \textit{with } n' \triangleq 2N-1-n \\
&= W_{2N}^{-k/2} \sum_{n=0}^{N-1} x(n) W_{2N}^{(n+0.5)k} + W_{2N}^{-k/2} \sum_{n=0}^{N-1} x(n) W_{2N}^{-(n+0.5)k} \\
&= W_{2N}^{-k/2} \sum_{n=0}^{N-1} 2x(n) \cos \frac{\pi k}{2N} (2n+1) \quad \textit{for } k \in [0, 2N-1]
\end{aligned}
$$

the last line following from $W_{N_2}^{-(n+0.5)k} = \exp(j2\pi(n+0.5)k/2N)$ and Euler's relation, which agrees with the original definition,eqn (4).

The formula for the inverse DCT, can be established similarly, starting out from

$$x(n) = \left[\frac{1}{2n} \sum_{k=0}^{2N-1} Y(k) W_{2N}^{-nk} \right] I_N(n).$$

DWT

Wavelet Transform has turned into an essential strategy for picture pressure. Wavelet based coding gives significant change in picture quality at high pressure proportions primarily because of better vitality compaction property of wavelet transforms [12]. Wavelets are functions which permit information investigation of signs or pictures, as indicated by scales or resolutions. The DWT speaks to a picture as a whole of wavelet functions, known as wavelets, with various area and scale. It speaks to the information into an arrangement of high pass (detail) and low passes (estimated) coefficients. The information is gone through arrangement of low pass and high pass channels. The yield of high pass and low pass channels are down inspected by 2.The yield from low pass channel is a rough coefficient and the yield from the high pass channel is a detail coefficient(Imran & Ghafoor 2012; Rani 2015). This method is one dimensional (1-D) DWT.but in this exploration work we are utilizing two dimensional (2-D) DWT. In the event of in two ways, the two lines and sections. The yields are then down examined by 2 toward every path as if there should be an occurrence of 1-D DWT. Yield is gotten in set of four coefficients LL, HL, LH 2-D DWT, the information is gone through arrangement of both low pass and high pass channel and HH.

[31]The image can have the extension such as JPEG, GIF, PNG etc. in case format of the image is analysed for attack detection than techniques is under the category of format based approach. JPEG image formats are generally used in this approach. Lossy compression causes statistical correlation between the pixels which is analysed using the quantization approach. In case image is compressed then it becomes difficult to detect the attack through format based approach.

Slant Let Transformation

[25]DWT is generally carried out by the use of filter bank transformation. However this technique cannot be used with time localization. In order to solve the problem time localization based slant let transformation can be used. This technique is advancement of DWT. At every scale or point of time different filters are used for enhancement of image. Octave band characteristics are retained using this transformation.

Camera Based approach

[14]As the image is captured from the capturing device such as camera, the image moves from capturing mechanism to memory card or any memory device attached with capturing mechanism. The sensors energy, capacitors and any other electronic circuit may be responsible for loss of information that is tackled using the camera based approach.

Physical Environment Based Approach

(Oommen n.d.)These techniques are based on interaction between physical object, light and the camera. Contrast analysis becomes a key issue in such environment. Contrast differs in case of physical environment analysis. Physical environment based approaches are easy to detect and rarely used to forge the image.

Geometry Based Approach

[10][21]In such approaches transformation alter the geometry of the image. The uniformity of the image is disturbed by the application of geometry of the image hence is easy to predict and detect. The detection process is easy hence this approach is also rarely utilized to forge the image.

Image encryption

This is now days commonly used mechanism in order to detect the attack within the image. Encryption of image is done in order to perform guard mechanism against the attacks. Parity bit is the commonly used encryption mechanism in which image is encrypted with special bits at particular positions. These positions are specified with power of 2. The formed codeword is transferred at destination end. At destination end decoders are placed in order to decrypt the image. This mechanism is employed in a region of heavy attacks.

II. LITERATURE SURVEY

Existing literature towards attack detection primarily concentrated towards physical security of images and torn down to content of images before allocation of encryption system is not considered. Thus complexity of detection is high. Study of existing literature is listed as under:

Noorjahan et al.[20]Solution Proposed by involving attack detection attack system combines the unique physical or behavioural traits to determine a person's identity. It is a pattern recognition system which includes feature extraction and comparison among these features against the template set in a database. Multimodal attack detection systems gather more than one trait for person recognition. These systems offer more accurate results in comparison to the unimodal systems so they are more popular, even though they are complex than unimodal system. In this paper an overview of the different multimodal attack detections system and the fusion techniques associated with them are explained. Discussion parts also include design issues, challenges and advantage of such systems over unimodal attack detection system.

Ahuja & Chabbra n.d et al. [2] discussed a attack detection technology was used to analyse human characteristics for the purpose of security. The fingerprint, hand, eye, face and voice are the most common physical attack detections patterns analyzed for security purposes. The main advantage of using attack detections is to verify a person's identity over using passwords or token. However, from the researches of past years it is concluded that the attack detection technologies can be defeated with low – tech and cheap materials. So it gives a new challenge to people and encouraged them to use multimodal attack detections as a means to enhance network security. In this paper we have discussed multimodal attack detections to increase the security level and with the fusion of multiple attack detections we can minimize the system error rates.

Mane n.d et al. [18]proposed a attack detection system to meet stringent performance requires high security applications. The fusion of multiple attack detections i.e. gathering of attack detections like figure prints, voice, iris helps in minimizing the system error rates. Fusion of multiple images causes difficulty for hackers to decrypt the information. More sophisticated methods are combined to scores from separate classifiers for each modality. This paper gives an overview of multimodal attack detections, the main research areas, challenges in the progress of multimodal attack detections and its applications to develop the security system for high security areas.

Gopal & Selvakumar et al. [9]in the development of recent technologies, a attack detections system has been the important affordable and more reliable system to provide network security to peoples. Biometric identification system is the automatic recognition of individual person based on their characteristics like voice, eyes retina, figure prints etc. Biometrics system is categorised in two broad areas namely unimodal attack detection system and multimodal attack detection system. In unimodal system only single attack detection system is used as sample so it has some disadvantage due to its lack of

non-universality and unacceptable error rate. But on the other hand multimodal is the better system for its two or three level of identification and verification. In this paper multimodal attack detections system characteristics are studied with its various attack detections traits and the comparison of different modalities is also processed to choose the best authentication mechanism. This paper performs multi attack detections system with its processing.

Shaikh 2016 in this age of digital impersonation, to prevent unauthorized access attack detection techniques are being used increasingly for authentication technique. The authentication through attack detections is done using individual's biological identities, and offer true proof of identity. The issues related to attack detections include security, forensics and remote managing. In this paper, unimodal, multimodal and fusion techniques are reviewed for authentication and extensive research has been conducted in this area with different techniques.

Panchal 2013 proposed paper security becomes a big requirement due to increase in crimes like computer hacking, illegal access of ATM & cell phone but security breaches in govt. and private buildings. These flaws become the advantage for criminals to break the security systems. For this attack detection recognition system are used for personal identification of every individual on the network. Biometrics of individual can`t be broken or hacked easily as compares to password, personal identification number, smart card etc. As advancement Multimodal system combines any number of independent attack detections and overcome some of the cons of unimodal attack detections. With the fusion of multiple attack detections system error rates can be minimized. This paper present overview of multimodal attack detections, challenges faced by multimodal attack detection system, applications to develop the security system for high security areas and application of attack detection systems and their advantage over unimodal attack detection system.

Aggarwal & Verma 2016 suggested multimodal attack detection systems provide more accuracy as compared to unimodal attack detection systems. Multimodal attack detection systems capture input from single or multiple sensors and measures two or more different modalities of attack detection characteristics. Multimodal attack detection technology uses more than one attack detection identifier to compare the identity of the individual person. The system can use three technologies i.e. face, mimic and voice. If one of the technologies is not able to give identity of the user, the system can still use another two to get accurate identify against user. This paper provides the study of various techniques used for performance enhancement, security and level of fusion in multimodal attack detection along with various challenges in multimodal attack detection.

Literature survey specific to copy move attack detection including pixel based approaches are discussed as under

Kaushik et.al 2015 proposed two dimensional discrete cosine transformation mechanism for attack detection. Adjacent pair of feature vectors is used to predict the copy move attack in digital images. The techniques presented gives better results in terms of PSNR and Accuracy. A copy move fraud is definitely not hard to make. The duplicated substance of picture which is used to perform fraud is called scrap. As the source and the target regions are from a similar picture, the photo features like confusion, shading, and edification condition et cetera will be same for the fabricated region and whatever is left of the photo. A sharp forger may similarly do some post-taking care of on the duplicated region like rotate, scaling,obscuring, tumult extension before the region is trapped.

Furon 2015 et al. [8] conducted the review of watermarking techniques used in order to detect attack within the image. This is a active approach in which prebuilt information is stored within the image and is detected in case of attack. The problem with this approach is complexity that can be minimised by replacing this mechanism with the pixel based approach.

Gupta 2012 proposed a watermarking mechanism for attack detection. Active mechanism is more complex as compared to passive mechanism however the complexity is reduced in this approach and accuracy of forged image detection is increased. Information in this case is scattered rather than embedding it inside a common frame.

Ma 2017 proposed digital copyright mechanism and its application for copy move attack detection. This is one of the most secure mechanism of transferring digital data however once forged this information

may not be recovered. Recovery of copyright information requires large amount of effort and hence intensive cost is encountered while using this approach and hence is rarely used.

Self-embedding et al. 2013 proposed a mechanism based on re-sampling for detecting image attack corresponding to image reconstruction. The reconstructed image correlation coefficient is analysed for corruption. In case problem detected the forged image is rejected in authorization process.

Ozdemir 2007, S, et.al. [22] data aggregation mechanism is used for analysing the data attack. Data aggregation mechanism stores the critical data at one place and hence attack can cause the distortion of that data. Copy move attack is common in such situation. In order to tackle the issue secure data aggregation mechanism is proposed through this literature.

Farid 2009, H et. al. [7] reviewed various image attack detection mechanism is conducted. The pixel based and splicing based mechanism is described. These mechanisms are said to be most commonly used mechanism for image attack detection. Another regular sort of video fraud is the face altering. It alludes to the sort of fabrication where a piece of the edge is reordered into another part, with the motivation behind including or erasing a question in the video outline. A few strategies are utilized for the discovery of this falsification and every one of them rely upon the suspicion that a face fabrication brings noteworthy connection between's the source outlines and copied ones

Das & Bhunre 2015 proposed a secure hashing mechanism for image attack detection. The detection process is based on pixel based approach. The forged image detection mechanisms are available however originator of this attack is not detected. In order to tackle the issue this approach was devices. Face assaults are credited to video as spatial and transient face imitation techniques. The previous is theoretically indistinguishable to the one in still picture outlines and includes the replication of a part of the casing. Then again, the last includes the supplanting of a few casings with a copy of earlier ones, keeping in mind the end goal to erase something in the scene of the first video. Halfway between outline assaults in the mean time, can be portrayed as a bit of a gathering of casings supplanted with a similar part from a picked video outline.

Tab.1|| Comparison of Techniques Used For attack Detection

Author	Title	Method	Advantages	Disadvantages
Noorjahan et. al.	Multimodal Biometrics: A Review	Fingerprint, voice, DNA, Face, Iris used for attack detections	Combines various modalities for identification and verification	Complex than unimodal
Mini Singh et. al.	A survey of multimodal attack detections	Fingerprint, hand, eyes, voice analyze	Increase the security level using multimodal attack detection, System error rate minimizes	Biometrics is vulnerable to attacks such as transmission, replay and spoofing.
Mane et. al.	Review of Multimodal Biometrics: Application, challenges and Research Areas	Fusion method	Integration of multiple sensors, optimal data is deliver	For more accuracy multimodal is used
Gopal et. al.	Multimodal Biometric Identification System An Overview	Comparison of different modalities	Improve matching performance of different samples	Lack of no universality and unacceptable error rate.
Shaikh et. al.	Review of Hand Feature of Unimodal and Multimodal Biometric System	Fusion techniques and review the different palm print & finger print techniques	Increase accuracy and reliability	False error rate can occur
Panchal et. al.	Multimodal Biometric System	Fusion of multiple attack detections	Minimizes error rate	Provides unmanned access control
Aggarwal et. al.	Multimodal Biometric Systems– A Survey	Face, mimic and voice are used as attack detection	More accuracy as compared to unimodal system	Improvement in matching performance is required

III. CONCLUSION AND FUTURE SCOPE

Image tempering causes loss of information that could be vital to the organization. Falsification is an issue and required to be tackled. For this purpose, attack detection mechanisms are provided. Procedures are required to be invented to detect the modification to the original image. Image attack

detection is one of the essential issues associated with the forensic science.

Then again, face attack confinement techniques that depend on outlines are suitable with outline identification duplication and not the restriction of manufactured district in the event that the content is reliable and the earlier adjusted area had bring down quality casings than the present edge. With regards to pixel-based methodologies, the control of identification exactness impacts post-handling and pressure and along these lines making the approval of execution measures (i.e. exactness, power, security) turns into a noteworthy concern inferable from the nonappearance of built up benchmarks and open testing dataset that assesses the real precision of advanced fraud approaches.

REFERENCES

[1] Aggarwal, A. & Verma, M.K., 2016. Multimodal Biometric Systems – A Survey. International Journal of Advanced Research in Computer Science and Software Engineering, 6(3), pp.437–441.

[2] Ahuja, M.S. & Chabbra, S., A Survey of Multimodal Biometrics. International journal of Computer Science and its Applications, pp.157–160.

[3] Das, T.K. & Bhunre, P.K., 2015. LNCS 8956 - A Secure Image Hashing Technique forattack Detection. , pp.335–338.

[4] Farid, H., 2009. Imageattack Detection (March), pp.16–25.

[5] Furon, T., 2005. A Survey of Watermarking Security., pp.201–215.

[6] Gopal, N. & Selvakumar, R.K., 2016. Multimodal Biometric Identification System - An Overview. International Journal of Engineering Trends and Technology (IJETT), 33(7), pp.351–355.

[7] Gupta, P., 2012. Cryptography based digital image watermarking algorithm to increase security of watermark data. , 3(9), pp.1–4.

[8] Imran, M. & Ghafoor, A., 2012. A PCA-DWT-SVD based Color Image Watermarking., pp.1147–1152

[9] Kaushik, R., Kumar, R. & Mathew, J., 2015. On Imageattack Detection Using Two Dimensional Discrete Cosine Transform and Statistical Moments. , 70, pp.130–136.

[10] Ma, Z., 2017. Digital Rights Management : Model, Technology and Application, pp.156–167.

[11] Mane, P.V.M., Review of Multimodal Biometrics : Applications, challenges and Research Areas, 3(5), pp.90–95.

[12] Oommen, R.S., A Survey of Faceattack Detection Techniques for Digital Images.

[13] Ozdemir, S., 2007. Secure and Reliable Data Aggregation for, pp.102–109

[14] Panchal, T., 2013. Multimodal Biometric System. International Journal of Advanced Research in Computer Science and Software Engineering, 3(5), pp.1360–1363

[15] Rani, S., 2015. Available Online at www.ijarcs.info Watermarking using DWT and PCA, 6(6), pp.117–120.

[16] Self-embedding, W. et al., 2013. Efficient Method for Content Reconstruction, 22(3), pp.1134–1147.

[17] Shaikh, J., 2016. Review of Hand Feature of Unimodal and Multimodal Biometric System. International Journal of Computer Applications, 133(5), pp.19–24

[18] Sheikh, Z.G. & Thakare, V.M., 2016. Wavelet Based Feature Extraction Technique for Face ecognition and Retrieval : A Review., pp.49–54