International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
***Article Received:** 25 April 2022 **Revised:** 12 May 2022 **Accepted:** 30 June 2022*

Battlefield Security: A Novel Facial Recognition Algorithm

[1]Ms. Sakshi Chhabra (Ph.D Scholar) [2]Dr. U. S Pandey(Principal at School of Open Learning)
[1]Mewar University [2]University of Delhi

ABSTRACT: In the modern era of rapid technological advancements, facial recognition has emerged as a pivotal tool for identifying faces from both static images and dynamic video feeds. This technology leverages nodal points of facial features and compares them with a database of images, operating primarily through Artificial Intelligence. This paper explores the implementation of facial recognition algorithms for real-time fraud detection on the battlefield. Two key algorithmic features, Liveness Detection and Local Binary Patterns (LBP), are highlighted for their effectiveness. To enhance national security and safeguard citizens, defines organizations worldwide are continuously seeking innovative methods to strengthen border security. This study relies on secondary data gathered from diverse sources to support its findings.

KEYWORDS- LBP, Live ness detection, real time, facial recognition

1. **INTRODUCTION**-

Globally, defense organizations enforce strict vigilance protocols on the battlefield, necessitating effective surveillance systems. Real-time automatic human tracking systems for restricted areas show significant potential to become the default security platform for border control worldwide. This paper analyzes two facial recognition algorithms—Liveness Detection and Local Binary Patterns (LBP)—highlighting their application in real-time scenarios. For instance, the French company ATOS, known for its exceptional Bull Battlefield Management System, still faces opportunities to enhance security measures with emerging technologies. Similarly, the Indian Army has deployed the PJT-531 Battlefield Surveillance Radar along the Line of Control (LOC) to bolster security. ROLTA, a Mumbai-based company, is also working on improving battlefield security systems. As technology evolves, it becomes imperative to adopt advanced methods to enhance accuracy and reliability in security systems.

1.1 Live Ness Detection Algorithm-

The objective of liveness testing is to decide if the biometric that is being caught is a real estimation from the approved, live individual who is available at the hour of capture. Liveness identification recognizes live people from introduction assaults, for example, photographs, recordings or veils.

1.1.1 Security-

3D cameras are being used for biometric ID. This permits frameworks to recognize when photos or imitations, including 3D printouts and veils, are being utilized. This innovation builds security without requesting any additional exertion from the user. Fraud avoidance is the primary motivation behind why liveness discovery is required for a safe facial confirmation application. The strategies that help alleviate parody related dangers, for example, counterfeit fingers, are intended to ensure unique mark sensors and lower the hazard for extortion. Liveness discovery virtual products builds the security of unique mark validation. (AI) makes it versatile to any type of ridiculing. The security level can be altered to work with a particular equipment configuration. Recognition and Liveness Detection – Liveness identification is utilized related to facial acknowledgment to identify whether somebody is deceitfully imitating another person, which should be possible either by wearing a prosthetic cover or introducing a lifeless photograph or picture.

1.1.2 Application-

Grin to pay (Alipay)- Ant Financial said the Smile to Pay innovation has arrived at a degree of exactness and security that should comfort Alipay clients. The multistep cycle of one to two seconds of facial checking utilizes a 3D camera and a "live-ness location calculation" to ensure a client's personality. For instance, the calculation can identify shadows and different highlights that can just originate from

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
***Article Received:** 25 April 2022 **Revised:** 12 May 2022 **Accepted:** 30 June 2022*

living creatures, along these lines blocking photographs or video that may be utilized by somebody attempting to seize an individual's Alipay account. The expansion of the telephone number check "further guarantees the security of exchanges," Ant Financial said.

1.1.3 User friendly

Liveness discovery stage decides this present reality adequacy of hostile to caricaturing innovation and gives better insurance to the clients. Better and Faster User Experience – The framework guarantees that genuine clients have straightforward, instinctive and low-grating experience.

1.1.4 Eye Blink Detection

Eye blink detection is one liveness identification test that is extraordinarily precise. Common squinting is a simple method to decide whether a face is live or not. The normal human flickers 15–30 times each moment. The eyes stay shut for around 250 milliseconds during a flicker. Current cameras record recordings with far littler stretches between outlines (50 milliseconds at 30 edges for every second).

1.2. LBP(Local Binary Patterns)-

LBP important property is its computational simplicity, which makes it possible to analyze images in challenging real time environment. The secure LPB features can be extracted by the server from these encrypted images. The secure LBP features can be used directly for many applications and retain the most characteristics of the original LBP features.

1.2.1 Security-

The brilliant grounds can screen understudies progressively by dissecting understudies' pictures, however an enormous number of pictures carry an agonizing weight to the keen grounds. The comfort of distributed computing has pulled in shrewd grounds to redistribute their gigantic measure of information to cloud workers. In spite of the fact that the redistributing of information can decrease the computational and capacity trouble on brilliant grounds, the security saving turns into the greatest concern.

1.2.2 Texture operator

Because of its discriminative force and computational effortlessness, LBP surface administrator has become a mainstream approach in different applications. The means required to accomplish this are:

- creating dataset
- face securing
- feature extraction
- classification

1.2.3 Accuracy-

The acknowledgment paces of the LBP keep up elevated level under the impact of restriction mistakes.

1.3 Battle field security

The accompanying viewpoints are shrouded in the 2 calculations with the goal that an improved proficient framework can be introduced for facial acknowledgment at war zone.

1.3.1 Data loss prevention

A key to information misfortune counteraction is innovations, for example, encryption and tokenization. They can secure information down to field and subfield level, which can profit an endeavour in various ways: Cyber-assailants can't adapt information in case of an effective penetrate.

1.3.2 The cloud

"The cloud will trans formatively affect the security innovation industry by and large," As more associations utilize the cloud for what has customarily been the space of on-premises IT, more ways to deal with security that are conceived in and for the cloud will show up. On-premises procedures will be progressed to the cloud. Things, for example, virtualized security equipment, virtualized firewalls, and virtualized interruption location and counteraction frameworks. In any case, that will be a halfway stage. With the assistance of Smart grounds in LBP Algorithm this issue is additionally disintegrated of distributed computing.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
***Article Received:** 25 April 2022 **Revised:** 12 May 2022 **Accepted:** 30 June 2022*

1.3.3 Automation

Deft improvement approaches utilize broad mechanization to assist engineers with making secure code and send that code. However in some cases organizations don't go far enough. Every running application and foundation ought to be routinely checked for security and consistence, and computerization can help there too.

1.3.4 Test and retest

Robotization ought not be restricted to testing code at advancement time and speeding the arrangement of utilizations. Post-arrangement testing is basic, as is ordinary security testing of cloud administrations by people.

1.4 Anti-spoofing techniques

The Most Popular Face Anti-Spoofing Techniques most of face satirizing assaults are known as introduction assaults. These assaults utilize 2D and 3D (static or dynamic) to trick facial acknowledgment software. Static 2D introduction assaults depend on photos, level paper, or veils, while dynamic renditions use screen video replays or a few photos in a sequence. Static 3D introduction assaults may utilize 3D prints, figures, or covers, while dynamic variants utilize advanced robots to repeat articulations, complete with makeup. Of course, these models are not a definitive truth. As advances advance, so do introduction attacks. Today — 2D is more well known than 3D because of innovative constraints.

1.4.1 Eye Blink Detection-

Eye flicker recognition is one liveness identification test that is unbelievably exact. Regular flickering is a simple method to decide whether a face is live or not. The normal human flickers 15–30 times each moment. The eyes stay shut for around 250 milliseconds during a squint. Current cameras record recordings with far littler stretches between outlines (50 milliseconds at 30 casings for each second)

1.4.2 The Challenge-Response Technique

Difficulties and reactions are another enemy of satirizing procedure that is reasonable. This strategy utilizes an extraordinary activity called a challenge. The framework attempts to check that the test happened during a video grouping. A test reaction framework depends on a progression of difficulties to approve a person's identity. These difficulties can include: Smiles, Facial articulations of pity or joy. Head developments, 3D Camera

1.4.3. 3D cameras are the most dependable methods for hostile to caricaturing. Exact pixel profundity data can give high precision against introduction assaults since we can differentiate between a face and a level shape.3D assaults can cause challenges, however cameras are as yet one of the most dependable face hostile to ridiculing methods accessible. Also, notwithstanding the accessibility of cameras, not all clients have them on their PCs.

1.4.4 Active Flash

Dynamic glimmer is an intriguing procedure that we feel shows a ton of guarantee. We chose to test it for our particular undertaking. Furthermore, in contrast to a portion of different arrangements — it doesn't experience the ill effects of the "discovery problem. “This arrangement permitted us to distinguish parodying utilizing light reflections on a face. The thought includes utilizing a changing light condition gave by the extra light that originates from a gadget's screen. The white light delivers a fitting reflection on the face.

2. OBJECTIVES

1) Identify features of facial recognition algorithms to improve security

2)To study the algorithms for real time application.

3. LITERATURE REVIEW

1) Lavanya Sharma(2019)- An Improved Local Binary Patterns Histograms Technique for Face Recognition for Real Time Applications-Recently, face acknowledgment and its applications has been considered as one of the picture investigation best applications, particularly in the course of recent years. Face Recognition is a remarkable framework that can be utilized by utilizing novel facial highlights for ID or confirmation of an individual from an advanced picture. In a face acknowledgment framework, there are numerous strategy that can be utilized. This paper gives an effective of the Local Binary Patterns Histograms (LBPH) based strategy gave by OpenCV library which is actualized in Python programming language which is well appropriate for practical situations. In this paper we likewise furnish visual subjective result with existing calculation (Haar-course classifier and Local Binary Patterns Histograms (LBPH)). Therefore, the proposed procedure outflank better regarding visual subjective examination.

2) B.Sree Vidya E.Chandra (2019) – Entropy based Local Binary Pattern (ELBP) highlight extraction strategy of multimodal biometrics as safeguard system for distributed storage Cloud Computing (CC) is an innovation that is developing significantly and has pulled in wide range of clients. The broad use of cloud innovation is impacted by different variables like convenience, pay-per use system, simple access, cost-viability and so on. In spite of the fact that it is a generally utilized innovation, challenges exist as security dangers. There are an assortment of administrations that are offered by cloud. These incorporate Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). Capacity is one of the key assistance contributions under IaaS. To give a protected advanced stage to clients to work with, this examination work proposes a novel security design for made sure about capacity in cloud that gives a strong confirmation by utilizing various biometric modalities.

3) Farah Deeba Hira Memon Fayaz Ali Dharejo Aftab Ahmed(2019)- LBPH-based Enhanced Real-Time Face Recognition-Facial acknowledgment has consistently experienced a reliable exploration region because of its non-demonstrating nature and its various applications. Accordingly, everyday exercises are progressively being done electronically as opposed to in pencil and paper. Today, PC vision is a thorough field that manages an elevated level of programming by taking care of the information pictures/recordings to naturally perform errands, for example, discovery, acknowledgment and order. Indeed, even with profound learning strategies, they are better than the ordinary human visual framework. In this article, we built up a facial acknowledgment framework dependent on the Local Binary Pattern Histogram (LBPH) technique to treat the constant acknowledgment of the human face in the low and significant level pictures. We seek to expand the variety that is applicable to outward appearance and open edges so to kind of encode edges in a modest manner. These profoundly fruitful highlights are known as the Local Binary Pattern Histogram (LBPH).

4) M. Ďulík* and M. Ďulík jr. (2019)- Cyber Security Challenges in Future Military Battlefield Information Networks-This paper clarifies the advancement of innovation from out of date military combat zone systems towards the worldwide military front line data organize from data and digital security perspective. The creators centre around the danger of the correspondence medium which is primarily utilized in military front line data systems – the remote channel, which is the premise of various versatile remote frameworks. This paper manages complex dangers to military the internet, wherein basically remote channels might be effectively accessible by the adversary. Utilized subnetworks may have various properties. A bringing together broadened layered model is introduced in the article, which notwithstanding ISO/OSI model spreads digital danger to geographic and social circles. The article additionally right away outlines the advancement of electronic military fighting towards digital military fighting.

5) Jung ho Eom(2015)- Security Threats Recognition and Countermeasures on Smart Battlefield Environment based on IoT- this paper, we drew new security dangers on IoT (Internet of Thing) based brilliant front line condition and proposed countermeasures against them. DoD (Department of Defense) is concentrating on the advancement of automated battle frameworks (UCS) to plan for future war. The IoT innovation gives organizing administration to associate each other automated battle framework. Be that as it may, IoT has the security weaknesses of every component of the innovation itself on the grounds that the innovation incorporates a few segments to arrange a particular help. What's more, new security weaknesses will be caused when they are interconnecting.

6) Saptarshi Chakraborty, Dhrubajyoti Das(2015) An Overview of Face Liveness Detection-

Face acknowledgment is a generally utilized biometric approach. Face acknowledgment innovation has grown quickly as of late and it is more straightforward, easy to understand and advantageous contrasted with different strategies. However, face acknowledgment frameworks are powerless against parody assaults made by non-genuine countenances. It is a simple method to parody face acknowledgment frameworks by facial pictures, for example, representation photos. A protected framework needs Liveness discovery so as to prepare for such parodying. In this work, face liveness location approaches are arranged dependent on the different sorts strategies utilized for liveness identification. This order helps understanding diverse satire assaults situations and their connection to the created arrangements. A survey of the most recent works with respect to confront liveness location works is introduced.

7) Enas A. Raheem(2019)- Insight on Face Liveness Detection: A Systematic Literature Review- To audit specialist's endeavors in light of the issue of parodying and liveness discovery, planning the exploration diagram from the writing review into an appropriate scientific classification, investigating the fundamental properties of the field,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
Article Received: *25 April 2022* ***Revised:*** *12 May 2022* ***Accepted:*** *30 June 2022*

inspiration of utilizing liveness identification techniques in face acknowledgment, and Problems that may limit the points of interest. We introduced an oppressed hunt on face acknowledgment with liveness discovery and its equivalents in four fundamental information bases: Web of science, Science Direct, Scopus and IEEE Xplore. We accept that these information bases are broadly comprehensive enough to cover the writing. The last number of articles considered is 65 articles. 4 of them where audit and study articles that depicted an overall outline about liveness recognition and hostile to ridiculing techniques. Since 2012, and notwithstanding of leaving a few zones unestablished and needs more consideration, scientists attempted to monitor liveness discovery in a few different ways. Regardless of what their class is, articles focused on difficulties that faces the full utility of hostile to mocking techniques and prescribed a few answers for defeat these difficulties. In this paper, various kinds of liveness location and face against ridiculing methods are examined to keep specialists refreshed with what is being created in this field.

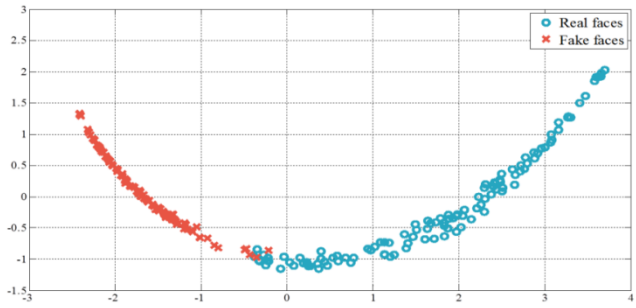
4. RESEARCH METHODOLOGY-

The study is based on secondary data. The required data has been extracted from various sources like research journals, periodicals, articles, government publications, magazines ,newspapers and authenticated websites.

5. DATA AND INTERPRETATION-

5.1 LIVE NESS DETECTION – SENSORS –

FIGURE 5.1



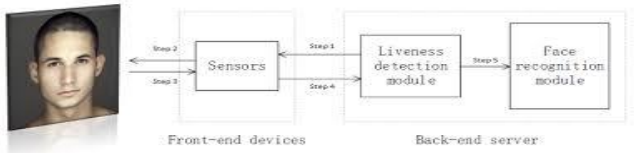
INTERPRETATION-

Figure 5.1. Principal component analysis (PCA)—Transformed features

Head part investigation (PCA) is applied to the aggregate dispersions and their agent eigenvectors are found. By anticipating the aggregate disseminations onto those eigenvectors, we can acquire new highlights and use them as edge highlights.

5.2) Architecture of face authentication system

FIGURE 5.2

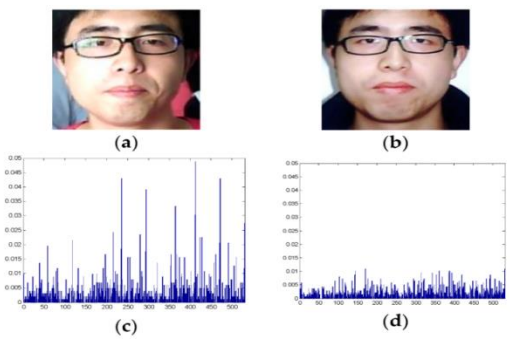


INTERPRETATION-

A typical architecture of face authentication system is illustrated in Fig 2 . It is divided into two parts: frontend devices and the back-end server. The front-end devices comprises camera and auxiliary sensors such as flash lamps, microphones. The back-end server contains two main modules: a liveness detection module and a face recognition module. When the user commences the authentication process, the liveness detection module is initiated and sends generated parameters to front-end devices (Step 1). Subsequently, the front-end devices synthesize challenges according to the received parameters and deliver them to the user (Step 2). After receiving the challenges, the user makes expressions, such as smiling blinking, as responses. The sensors in the front-end devices capture such responses and encode them (Step 3). Either in real time or in post processing, the front-end devices send the captured responses to the liveness detection module in the back-end server (Step 4). The liveness detection module gathers all decoded data and checks whether the user is an actual human being. If so, the liveness detection module selects some faces among all the responses and delivers them to the face recognition module to determine the identity of the user (Step 5).

5.3 Deviated textures in live and spoofing face images

FIGURE 5.3



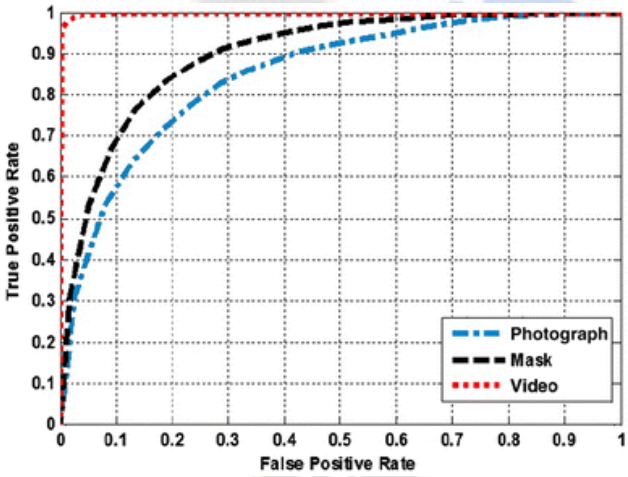
International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
Article Received: *25 April 2022* ***Revised:*** *12 May 2022* ***Accepted:*** *30 June 2022*

INTERPRETATION

Figure 5.3 presents a graphical portrayal of the R–G digressed surfaces in live and mocking face pictures, where the y hub means the level of deviation between the red and green channels. As uncovered by the figure, the surface contrast among red and green diverts in the live face picture is bigger than that in the caricaturing face picture. As it were, ridiculing face pictures present an alternate surface dissemination contrasted and that in live face pictures, which recommends that the R–G strayed surface might be an element with the capacity to separate among live and mocking face images. Figure 3 . R–G digressed surface in (an) a live face picture and (b) a parodying face picture; (c,d) Graphical portrayal of the R–G strayed surface in the live and caricaturing pictures.

5.4 Receiver operating characteristic- Liveness detection

FIGURE 5.4

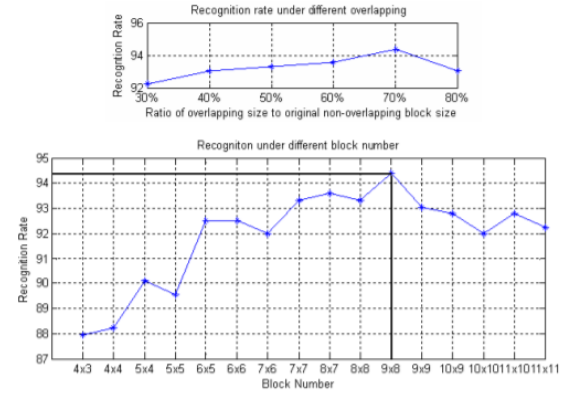


INTERPRETATION

Figure 5.4 shows the beneficiary working trademark (ROC) bends [28] for consolidated collinearity and colocation highlights utilizing the proposed combination conspire. The framework showed a close ideal exhibition on account of video assault recognition for a scope of FPRs. The presentation of the framework for veil assault identification was insignificantly better than that accomplished for photo assault discovery. ROC bend utilizing whole element vector In request to set up the compromise between the component dimensionality and liveness location, a forward element choice technique [14] was utilized. The element determination strategy was run multiple times with arbitrary arrangements of information for preparing and testing.

5.5 Recognition with LBP − TOP u2 8,8,8,3,3,3 under different overlapping sizes (top) and number of blocks (bottom).

FIGURE 5.5

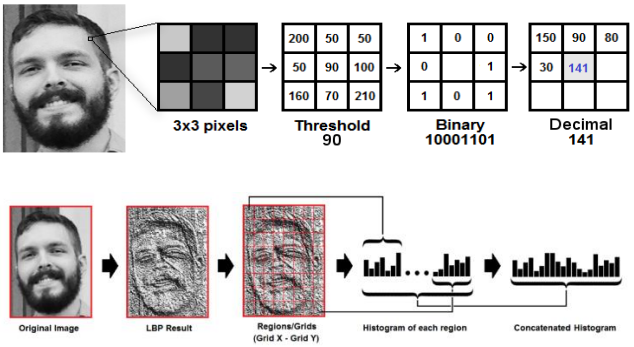


INTERPRETATION

The presence of DT can help enormously in acknowledgment, yet the presence of a face incorporates both personality and appearance data, which could make precise demeanor order more troublesome. Highlights from the XT and YT planes clarify more about the movement of facial muscles. Subsequent to trying different things with various square sizes and covering proportions, as appeared in Fig. 17, we decided to utilize 9 × 8 squares in our trials. The best outcomes were acquired with a cover proportion of 70% of the first non-covering square size. We utilize the covering proportion with the first square size to change and get the new covering proportion. Assume the cover proportion to the first square width is ra, subsequent to modifying, the new proportion is ra′ , and the accompanying condition speaks to the ra′ in stature.

5.6 Step-by-Step- explanation of the LBPH algorithm

FIGURE 5.6



INTERPRETATION-

1.First of all, we have to characterize the boundaries (sweep, neighbours, lattice x and framework y) utilizing the Parameters structure from the lbph bundle. At that point we have to call the Init work passing the structure with the boundaries. In the event that we not set the boundaries, it will utilize the default boundaries as clarified in the Parameters area.

2. Secondly, we have to prepare the calculation. To do that we simply need to call the Train work passing a cut of pictures and a cut of names by boundary. All pictures must have a similar size. The names are utilized as IDs for the pictures, so on the off chance that you have more than one picture of a similar surface/subject, the marks ought to be the equivalent.

3. The Train capacity will initially check if all pictures have a similar size. On the off chance that at any rate one picture has not a similar size, the Train capacity will restore a blunder and the calculation won't be prepared.

4. Then, the Train capacity will apply the essential LBP activity by changing every pixel dependent on its neighbours utilizing a default span characterized by the client. The essential LBP activity can be found in the accompanying picture (utilizing 8 neighbours and range equivalent to 1

5. After applying the LBP activity we extricate the histograms of each picture dependent on the quantity of frameworks (X and Y) passed by boundary.

6. The pictures, names, and histograms are put away in an information structure so we can contrast every last bit of it with another picture in the Predict work.

7. Now, the calculation is now prepared and we can Predict another picture.

8. To foresee another picture we simply need to call the Predict work passing the picture as boundary. The Predict capacity will extricate the histogram from the new picture, contrast it with the histograms put away in the information structure and return the name and separation comparing to the nearest histogram if no blunder has happened.

6. CONCLUSION-

Our study revealed that LBP and Liveness Detection are two algorithms that will improve the efficiency in real time in battlefield. Also in today's scenario security is a major concern for all the individuals. Privacy is also a crucial factor in battlefield management systems to prevent data loss. Although Atos and Rolta are existing companies which provide an efficient battlefield management system but with advancement in technology, recognition gets improved. When it comes to developing solutions for this problem, we believe it's important to focus on techniques that: Prevent static and dynamic 2D spoofs, Use images, not videos, Required no interaction from the user. A reliable solution needs to achieve maximum accuracy, require little time, and prioritize the user experience. Most importantly, it needed to integrate with existing facial recognition software. The two algorithms will give a one plus advantage for the smooth functioning of battle field management system as they are specialised in fraud detection and data loss prevention. The future scope is to enhance the facial recognition process by using algorithms like Adaboost etc.

REFERENCES-

1) Lavanya Sharma(2019)- An Improved Local Binary Patterns Histograms Technique for Face Recognition for Real Time Applications, International Journal of Recent Technology and Engineering 8(2s7):524-529 · September 2019 -
2) B.Sree Vidya E.Chandra (2019) - Entropy based Local Binary Pattern (ELBP) feature extraction technique of multimodal biometrics as defence mechanism for cloud storage Alexandria Engineering Journal, Volume 58, Issue 1, March 2019, Pages 103-114
3) Farah Deeba Hira Memon Fayaz Ali Dharejo Aftab Ahmed(2019)- LBPH-based Enhanced Real-Time Face Recognition- International Journal of Advanced Computer Science and Applications 10(5) · January 2019
4) M. Ďulík* and M. Ďulík jr. (2019)- Cyber Security Challenges in Future Military Battlefield Information Networks , Advances in Military Technology , Vol. 14, No. 2 (2019), pp. 263-277 ISSN 1802-2308, eISSN 2533-4123 DOI 10.3849/aimt.01248
5) Jung ho Eom - Security Threats Recognition and Countermeasures on Smart Battlefield Environment based on IoT- International Journal of Security and its Applications 9(7):347-356 · July 2015
6)) Saptarshi Chakraborty, Dhrubajyoti Das(2015) An Overview of Face Liveness Detection- Face recognition is a widely used biometric approach- International Journal on Information Theory (IJIT), Vol.3, No.2, April 2014
7) Enas A. Raheem- Insight on Face Liveness Detection: A Systematic Literature Review(2019)-International Journal of Electrical and Computer Engineering 9(6)