Review on Security Enhancement using Image Processing

Anita Kataria[1] & Rajendra Kachhwaha[2]
[1]Dept. of Cyber security, Sardar Patel University of police, security and criminal justice, Daijar, Jodhpur, Rajasthan, India.
[2]Dept. of Computer Science & Engineering, M. B. M. Engg. College, Jodhpur, Rajasthan, India.

Received Dec. 11, 2017 Accepted Jan. 16, 2018

ABSTRACT *Image and video processing perform a primepart in the growth of technologies for administer with reliabilityaffairsThere has been endless stuff of misuse that have remains in banking transactions. Hence it is verynecessary to bring high security in banking sector. This paper proposes the confederation of Face Recognition System in the distinctivenessauthentication procedureused in ATMs to intensify the security system. Supervision cameras are extensively used as way of enormity minimization, and image examination techniques are used in the forensics domain. With the help of image stitching and image steganography, security will be given to any likeness.*

Keywords: *image stitching, image steganography, skimming, four-frame differencing.*

I. INTODUCTION

Everyday operations are progressively being knobcomputerized.This expansion in digital transactions out-turn in hugerequirement for quick and exactcustomerrecognition and verification.Access codes for cipher, banks accounts and digitalorganization are generallyholds PINs for recognition and reliabilityclear-out. With the use ofgenuine PIN, we canhold access, but the customer of the PIN is not authorized. In case credit and debit cards are misplaced or stolen, an unverifiedcustomergenerally come with the properPIN. Face recognition technology canresolvesuch issues as face is certainlyallied to its holder in some situation of lookalike.

The growth of automationcarriesvariety of tools whichgives much user satisfaction. Now to make banking offhand for users' ATM machines are used. Although it has somebenefits and drawback. Recently ATMs make benefit of access card and PIN for singularity acceptance. Using Face Recognition System,it can be detecting number of falseeffort and misconductover card and PIN theft, stealing and hacking of users account specifics and other chunk of security.

II. WHY WE NEED SECURITY

Skimming is one of the trendyway of ATM attack calculated for 80% of ATM fraud. Along with this Cash and Card Trapping, Pin Compromise, System Attacks are some reasons which breach the security. U.S. banks costs an average of $15,000 ATM fraud each year.RecentATM authorization schemes are bounded to access cards and PINs.A total of 114 ATM attacks were reported in EUEROPEAN, up from 28 during 2016, 30.7% increase. 'Black Box' is the connection of invalidation device which sends allotted command straight to the ATM cash merchant to 'cash-out' the ATM. Relevant damagewas up 268%, from €0.41 million to €1.51 million.

EUROPEAN PAYMENT TERMINAL CRIME REPORT STATISTICS - SUMMARY

Terminal Related Fraud Attacks	H1 2013	H1 2014	H1 2015	H1 2016	H1 2017	% +/- 16/17
Total reported Incidents	12,676	7,345	8,421	10,820	11,934	+10%
Total reported losses	€124m	€132m	€156m	€174m	€124m	-29%%
ATM Related Physical Attacks	H1 2013	H1 2014	H1 2015	H1 2016	H1 2017	% +/- 16/17
Total reported Incidents	1,007	1,032	1,232	1,604	1,696	+6%
Total reported losses	€10m	€13m	€26m	€27m	€12.2m	-55%
ATM Malware & Logical Attacks	H1 2013	H1 2014	H1 2015	H1 2016	H1 2017	% +/- 16/17
Total reported Incidents		20	5	28	114	+307%
Total reported losses			€0.14m	€0.41m	€1.51m	+268%

Source: European Association for Secure Transactions (EAST)

Fig 1 summary of European payment crime report

[EAST Publishes European Fraud Update 3-2017](#)
Posted on 09/11/2017

III. DIGITAL IMAGE PROCESSING

An image is deliberate to be anequation of two real variables, for example, let (P, Q) with "a" as the amplitude (e.g. brightness) of the image. (P, Q) is real coordinate of the image.An image is apprised to have sub-images consider as regions-of-interest, ROIs. Everycomponent of the matrix, pixel, is used to represent an intensity.The whole procedure of Image Processing is segmented into three domains

(i) Discretization and representation:modifying visual instructions into a distant form which isadaptable for computer procedures toprotectmemory space and time necessity in succeeding processing.

(ii) Processing:advancing image standard by filtering and compressing information to keep storage and channel quantitywhile transmission.

(iii) Analysis: drawing out image characteristic,certifying aspect, analysis and identification.

IV. FACE RECOGNITION SYSTEMS

Face Recognition System is autilization that automaticallyreorganize a user from ananalog image or a video blueprint from a video origin. In this processthere is choiceof facial features recognition from a facial storage and the image.Facial Recognitionneed no tangiblecommunication on side of the user. It is authentic and grant for hugeenlistment and authenticationlevel. It mayutilizeourcurrent hardware atmosphere, cameras and image acquisition.System will process without any issues.

V. WHEN DID IT DEVELOP?

All along 1964 and 1965, Bledsoe, Helen Chan Wolf and Bisson, worked on accepting the computer to be usual with personal faces. He was grandiose of his work, although the support was given by an anonymouscouriertam which did not permitmuchadvertisement, a bit work was announced. In period of the correspondframe to the feature of result in the database, the success of the process can be better. But the identificationissue was kept critical hard through the rotation, lighting intensity and angle, facial expression, etc. the work was followed foremost by Peter Hart. Peter's experiment in 1966, completed on a database reviews over 2000 images. Toreorganize thecharacteristics (such as eyes, ears, nose and mouth) on the photographs the first semi-automated system for face identification was made in 1960s. In 1970s,Goldstein and Harmon took 21 particular features like eye color and hair to digitalize the identification. The enhancement time for face identification was initiated in the delayed 1980s and they were present devices was made workable in the 1990s. In 1988, standard linear algebra technique, to the facial recognition was used by Kirby and Sirovich.

VI. HOW DO THEY WORK?

A database of user's face is managedthrough the devicewhichgrip face recognition. If a face requires to be anticipate a picture of the someone'sappearance is captured and examine to the lookexist in the database to onlooker if a rival is found. There are mainly 3 sectionsrelevant to a face recognition system: Face detector, Eye localizer and Face recognizer.

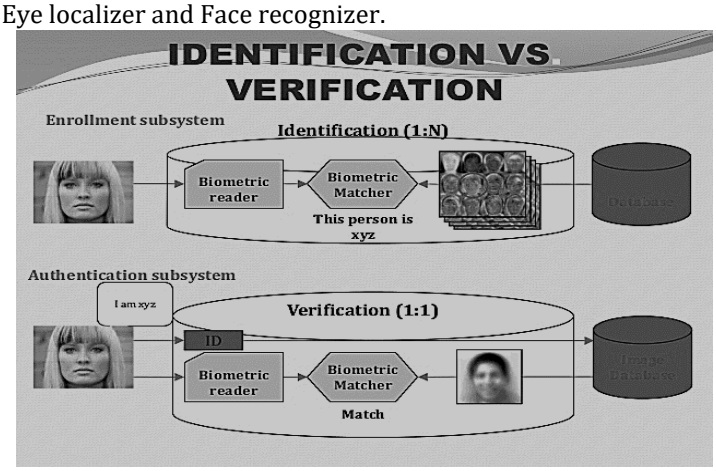

Fig 2 identification and verification
Published on Sep 5, 2013

security of ATM by image processing

In Facial identification there are two types of comparisons: -

VERIFICATION- The techniquesanalogize the particular personto whomit can be said they are and provide a yes or no conclusion.

IDENTIFICATION- The device analogizes the particular person to Other persons in the database and provide a remarked list of duplicates.All recognition or verificationtoolsrunthrough the four phases. First is Capture in which areal or behavioralexample is takenthrough the system whileenlistment and also in recognition or

authentication procedure. Second is specialinformationwhichdistillation from the fragmentation and anarrangement isgenerated. Third is Comparison in which the arrangement is then corelated with anotherarrangement. And last is Match/non-match through which the devicedetermineswhether the charactersdetected from anotherarrangement are a similar or a non-similar.

VII. IMPLEMENTATION

The implementation of face Identificationautomationcarry the below four phases:Image receiving, Image processing, Distinguishfeature location, Template generation, Template matching.

1. Image acquisition: Face-recognition tools can collectsample from any stationary camera or video device that creates images of enoughaspects and resolution. Good-quality acceptance is necessary to doauthentication and recognition.
2. Image Processing: sample are modified such that the facesampleremain same, and colorfulpictures are generally followed by black and white in to initiate comparisons based on grayscale features. The existence of faces or face in a frameshould be recognize. If the face is recognized, it should be confine and stabilization procedurecan be needed to conduct the dynamics of the live face sampling in adjustment with the one on the device.
3. Differentfeature location: All face-scan devicestry to testdetectable facial character in a mannersame to the fashion humandetecteach other. The charactersgenerallyused in facial-scan devices which isvery bitsimilar to modifyon frame.
4. Template creation:enlistmentsamples are generallygenerated from a profusion of facial template. These samples can differ in content from below 100 bytes, created by some vendors. The 3K template is one of the biggesttechnology among other which determine physiological biometrics. Many sample are generallyrelated with behavioral biometrics.
5. Template matching: A number of images is captured and remarkedacross the enlistment, so that a person trying 1:1 authentication within a face-scan device may have 10 to 20 try in 1 to 2 seconds. facial-scan is not soimpressive as finger-scan or iris- scan in recognizing a person from a hugestorage.

VIII. RECOGNITION SOFTWARE

When the device is fixed to a video examine system, the identification software tries to find the area of vision of a video camera for samples. If there is a sample like face is in the camera vision, it is recognizingin a part of a second. To find faces in poor resolution A multi-scale algorithm is used. The deviceturns towards a high- resolution examination only if a shape like head is recognize. If a face is recognized, the deviceresolve position, size and pose. A face has to be at 35 degrees in front of the camera for the device to capture it.Normalization process is conductwithout concerning of the location and distance from the capturing device. Light does not affect the procedure. The device converts the information into a different code. This procedure permits for flexibledifferentiation of the novelacceptedinformation to keepthe data. The accepted information is matched to the preexistinginformation. The device frames the face and generates a faceprint, anexclusive code for thesample. If thedatabase has keep a faceprint, it can corelate it to the numbers of faceprints kept in a system.

IX. WORKING OF FACE RECOGNITIONS SYSTEM IN ATM

In the ATMs, Face Recognition Systems (FRS) works in the successive way.firstly, the users image is capturedduring the account is unclosed and the customer is permitted to haveunauthorizedsamplingrestrictions. In ATMs, cards and PIN are used to identifycustomer. Customer picture is captured and try to compare it to the image stored in database. In case the caparison becomes true, it will permitfor further process. But if the comparison proves to be wrong, it restricts the provided transection. If acomparison issuccessful with the PIN but not with the image present in database, the bank canrestrict the process and keep the image of the customer for futureanalysis by bank official. Using credit card at ATMs, authenticationtemplatecould not perhapswithoutgenerating a safe side for the whole credit card providers.

X. DOES ALL ATMs SUPPORT FRS?

Mostly ATMs support Windows CE, 2000,XP Embedded, or Linux and these systems can flexible with facial recognition software. It has seen observed that both LocalFeature Analysis (LFA) and Principle Feature Analysis (PFA) programs candealwith changes. Thisis perhapsbecause withor without artificial illumination ATM is work for 24 hours.Authorizationphasescould beas uplift as 90% with the fact that FAS are looked after.

XI. FACTORS TO BE CONSIDERED

There are some aspectswhich canalter procedure.
These are:

1. Brightness
2. intensefacial definition
3. Dynamic of observation
4. Facial structure
5. Eye frames

Another thingisstoring the time above in the
Authentication procedure to few chunk, permitting for an advisable stage of authentication in a user's face whenmatch to the systemimage, and the cards
which areused at ATMs to draw backmoney are often given by organization, these organization do not have individualcommunication with the user, and thus no possibility to haveimage. The last issue is that user may be concernof the privacy issuesupraised by managingimages of users in anorganization record, becauseof probabilityof cyber-attacks or staff workers misconduct.

XII. CONCLUSION

Facial recognition software is used to getrequiredcomparisonremarks for utilizing ATM transactions process. Enhancing facial recognition systems to the identificationacceptance procedure used in ATMs mayovercomefalsebanking procedures to a highrange. Moving objects detection in frame string, is a basic requirement in video examination procedures. No doubt, present techniques do very well on videos surveillance by static cameras, but these ways fail when we talk about dynamic cameras. Specially, in poor frame quality and immediate brightness change differential, for exampleWide Area Motion Imagery (WAMI). We generally use three-frame differencing techniquefor object detection but it has some limitation in certain scenario. Then, a new enhanced technique was proposed a pixel-level algorithm based on four-frames differencing, in which the temporal data is required to differentiate the moving objects from the background effectively.

REFERENCES

[1]. Suganya, Nithya, Sunitha, MeenaPeethi, "SECURING ATM BY IMAGE PROCESSING – FACIAL RECOGNITION AUTHENTICATION"*International Journal of Scientific Research Engineering & Technology (IJSRET),* ISSN 2278 – 0882 Volume 4, Issue 8, August 2015.

[2]. Penev and Atick, Joseph J. "Local Feature Analysis: A General Statistical Theory for ject Representation." Network: Computation in Neural Systems, Vol. 7, No. 3, pp. 477-500, 1996.

[3]. Gross, Ralph, Shi, Jianbo, and Cohn, Jeffrey F. "*Quo vadis Face Recognition*." *Third Workshop on Empirical Evaluation Methods in Computer Vision*. Kauai: December 2001

[4]. Bone, Mike, Wayman, Dr. James L., and Blackburn, Duane. "*Evaluating Facial Recognition Technology for Drug Control Applications*." *ONDCP International Counterdrug Technology Symposium:* Facial Recognition Vendor Test., June 2001.

[5]. S. Sruthy. "Literature Survey Automated Person Identification Techniques.", *international journal of computer science and mobile computing (IJCSMC),* Volume 2, Issue 5, pp 232-237, May (2013).

[6]. Ahmed Abdelli and Ho-Jin Choi, "A Four-Frames Differencing Technique for Moving Objects Detection in Wide Area Surveillance", *Big Data and Smart Computing (BigComp), IEEE International Conference*, 2017.

[7]. J.S.V. Suresh Kumar,Face recognition, 2013.https://www.slideshare.net/gsantosh031/face-recognition-ppt accessed on 20 January, 2018.

A wise man gets more use from his enemies than a fool from his friends.

~ Baltasar Gracian