A Pixel Based Signature Authentication System

A. Vinoth, V. Sujathabai

Abstract- Signature verification is the process used to recognize an individual's h a n d -written s i g n a t u r e . The p r o c e s s o f verifying signature is cumbersome in practice. There is a need for automatic verification system for a signature since the signature has been a means of a person's identification through ages. Verification of a signature can be done either Offline or Online based on the application. Online systems use dynamic information of a signature captured at the time the signature is made. Offline systems work on the scanned image of a signature.

In this paper, we verify the off-line signatures by taking a boundary of the entire signature and do the pixel comparison. Signature is acquired using a scanner. Detection process is done after the data acquisition and pre-processing. Pre processing includes noise removal, grey-scale, manipulation, edge detection. Experimental results show that 50% of the accurate matching with the existing one from the data base.

Signature is a behavioral biometric: it differs from finger print, face, iris recognition, because these are based on the physical properties of human beings. There is an important distinction between simple signature Comparisons and dynamic signature verification. Both can be computerized, but a Simple comparison only takes into account what the signature looks like. Dynamic signature verification takes into account how the signature was made. With dynamic signature verification it is not the shape or look of the signature that is meaningful; it is the change in speed, pressure and timing that occur during the act of signing. Only the original signer can recreate the changes in timing and X, Y and Z (pressure).

A pasted bitmap, a copy machine or an expert forger may be able to duplicate what a signature looks like, but it is virtually impossible to duplicate the timing changes ins X, Y and Z (pressure). The practiced and nature motion of the original signer would require repeating the pattern shown. There w i l l al ways be sli ght vari at i ons in a Person's hand-written signature, but the consistency created by natural motion and practice over time creates a recognizable pattern that makes the hand-written signature a natural for biometric identification.

Signature v e r i f i c a t i o n i s n a t u r a l a n d i n t u i t i v e . The technology is easy to explain and trust. The primary advantage that signature verification systems have over types of biometric technologies is that signatures are already accepted as the common method of identity verification. This history is trust means that people are very willing to accept a signature based verification system.

Key Words: Pre-processing, data acquisition, off-line signature, edge detection, noise removal, gray-scale manipulation.

Manuscript received May, 2013.

Mr. A. VINOTH, MCA, M.Phil, [Ph.D], Assistant Professor's Department of Master of Computer Applications Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College Chennai, India.

Mrs. V. SUJATHABAI, MCA, M.Phil, [Ph.D]., Assistant Professor's Department of Master of Computer Applications Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College Chennai, India.

I. INTRODUCTION

Signature verification is the process used to recognize and individual's hand written signature. The process of verifying signature is cumbersome in practice. This is due to the fact that signature is a behavioral biometric: it differs from fingerprint, face, iris recognition, because these are based on the physical properties of the human beings.

Dynamic signature verification technology uses the behavioral biometrics of a hand written signature to confirm the identity of a computer user. Ammar et al. [3] who were one of the earliest researchers to extract "dynamic" information from a static image for signature verification.This i s a c c o m p l i s h e d b y anal yzing t h e speed, shape, stroke, and pen pressure and timing information during the act of signing. As a replacement for a password or a PIN number, dynamic signature verification is a biometric technology that is used to positively identify a person from their handwritten signature.

There is an important distinction between simple signature comparisons and dynamic signature verification. Both can be computerized, but a simple comparison only takes into account what the signature looks like. Dynamic signature verification takes into account how the signature was made. With dynamic signature verification it is not the shape or look of the signature that is meaningful; it is the changes in speed, pressure and timing that occur during the act of signing. Only the original signer can recreate the changes in timing and X, Y and Z (Pressure).

A pasted bitmap, a copy machine or an expert forger may be able to duplicate what a signature looks like, but it is virtually impossible to duplicate the timing changes in X, Y and Z (pressure). The practiced and natural motion of the original signer would require repeating the patterns shown.

There will always be slight variations in a person's handwritten signature, but the consistency created by natural, but the consistency created by natural motion and practice over time creates a recognizable pattern of biometric identification. Signature verification is natural and intuitive. The technology is easy to explain and trust. Takagi- Sugeno (TS) model is used to detect the forgery detection of off- line signatures using fuzzy logic [1, 2]. The primary advantage that signature verification systems have over other types of biometric technologies is that signatures are already accepted a s t h e c o m m o n m e t h o d o f i d e n t i t y verification. This history of trust means that people are very willing to accept a signature based verification system.

Dynamic signature verification technology uses the behavioral biometrics of a hand written signature to confirm the identity of a computer user. Another survey article [5] has been summarized the approaches used for off-line signature verification from 1993-2000. Unlike the older technologies of passwords and keycards which are often shared or easily forgotten, lost and stolen dynamic signature verification provides a simple and natural method for increased computer

security and trusted document authorization. A fully automated computerized system would avoid these problems to a maximum level.

II. PROPOSED SYSTEM

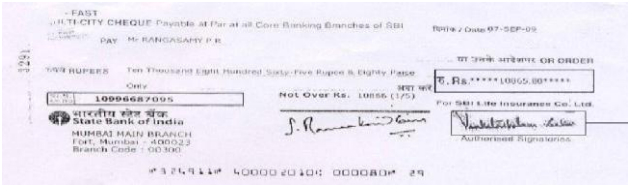
This paper deals with verifying the off-line signature in cheques. Many met hods a r e c u r r e n t l y avai l abl e f o r verifying the off-line signature. We have come out with a approach, which makes a pattern comparison of pixels captured within a specified boundary of signature. Figure2 shows the steps involved in our system.

After acquiring the signature from the user, it has to undergo the above steps (preprocessing stages) in order to get a g o o d q u a l i t y i mage . A s c a n n e r d i g i t i z e s t h e signature in 256 gray levels with 400 dpi resolution and the images are stored in tagged image file format. A specimen copy of 20 signatures is acquired from each individual customers and it is stored in the database.

III. STAGES IN PRE- PROCESSING

Pre- processing is to develop a clear and good clarity images. Pre-Processing stages consists of normalization, gray- scale manipulation, edge detection and noise removal. Normalization is used to have images of fixed size. If the sizes of the images are different, comparison becomes tedious process. Gray-scale manipulation is an intensity mapping method in which each pixel is assigned a gray value to improve the contrast of the images. Edge detection is adopted in order to make sure the complete image is taken into consideration. Noise, which has been defined as unwanted information in an image.

IV. VERIFICATION



Signature enclosed within the boundary

Figure. 1 Shows a Sample Cheque

Step1: get the processed signature image **Step2:** Assign count = 0; matched image= 0
Step3: Compare the processed signature images with the corresponding customer's image in the data base.
Step4: Comparing pixels of both the images. If both corresponding pixels matched, then increment the count value.
Step5: Consider the next pixel and go to step 4 **Step6:** Repeat steps 4 and 5 until all the corresponding pixels are matched.
Step7: If the pixel comparison is greater than 50 percentage, then increment counter value of matched image.
Step8: If the matched image is greater than or equal to 10 then accept signature is correct. **Step9:** If the matched image is less than 10, then accept signature is incorrect.

V. IMPLEMENTATION AND RESULT

Each customer shall have their sample signatures recorded and stored in the database. The images are stored in JPG format. The extraction of a signature from a bank cheque is a difficult task [7] as the cheque backgrounds are complex in nature. The cheques are scanned and compares with the signature of his/her database and comes out with a result. Signature in the cheques is compared with that of the existing database signature of that particular. Since we have 20 specimen signatures of the same person, we have wider area of comparison. We have limited that, if 10 of them matches, then we accept else reject it. We have implemented in MATLAB

VI. CONCLUSION

Signature scan has several strengths. Because of the large amount of data present in a signature scan template, as well as the difficulty in mimicking the behavior of singing, signature scan- technology is highly

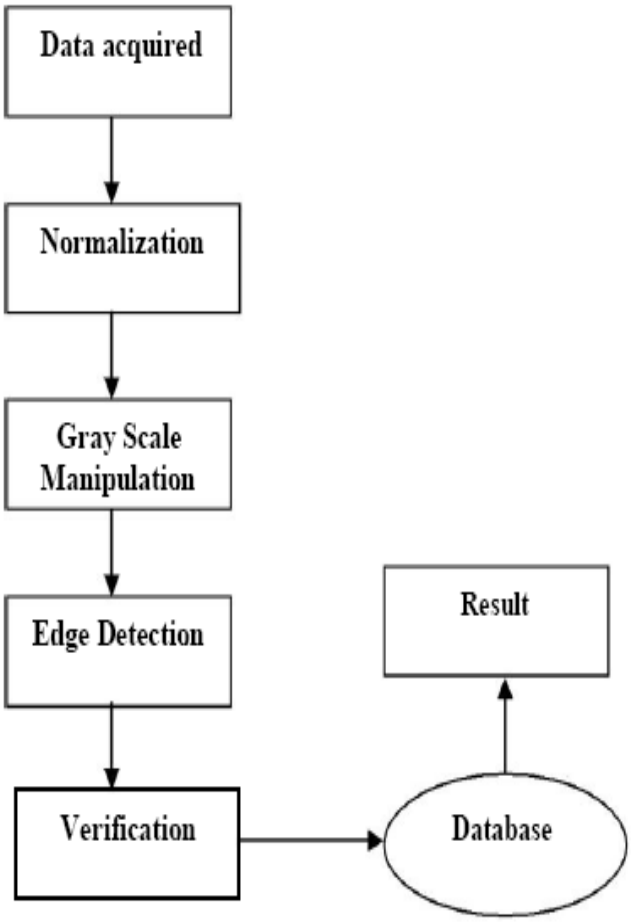


Figure – 2: Steps involved in the System

to be. Signature – scan also benefits from its ability to leverage exiting processes and resistant to imposter attempts. As a result of the low false Acceptance Rate (FAR), a measure of the likelihood that a user claiming a false identity will be accepted, deploys can have a high confidence level that successfully matched users are who they claim

hardware, such as signature capture tablets and systems based on public key infrastructure (PKI), a popular method for data encryption. Since most people are accustomed to providing their signature during customer interactions, the technology is considered less invasive than some other biometrics.

However, signature- scan has several weaknesses. A pseudo- outer product- based fuzzy neural network drives the signature verification system [6]. Signature – scan is designed to verify subjects based on the traits of their unique signature. As a result, individuals who do not sign their names in a consistent manner may have difficulty enrolling and verifying in signature-scan. During enrollment subjects must provide a series of signatures that are similar enough that the system can locate a large percentage of the common characteristics between the enrollment signatures. For the purpose of signature detection and verification of forgeries TS model is used in the existing methods [8, 9]. During verification enough characteristics must remain constant to determine with confidence that the authorized person signed. As a result, individuals with muscular illnesses and people who sometimes sign with only their initials might result in a higher False Rejection Rate (FRR), which measures the likelihood that a system will incorrectly reject an authorized user. Since many users are unaccustomed to signing on a tablet, some subjects' signatures may differ to their signatures on ink and paper, increasing the potential for false rejection.

REFERENCES

[1] M. Ammar, Y.Yoshida, T. Fukumura, "A new effective approach for offline verification of signature by using pressure features",In Proceedings of the International Conference on Pattern Recognition, pp 566-599,1986.
[2] S.Djeziri, F.Nouboud, R.Plamondon, Extraction of signatures from check background based on a filiformity criterion, IEEE Trans.Images Process.7 (10) (1998) 1425-1438.
[3] MadasuHanmandlu, Mohd.Hafizuddin, Mohd.Yusof, Vamsi Krishna Madasu, Offline signature verification and forgery detection using Fuzzy Modeling, Pattern Recognition 38 (2005) 341-356.
[4] M.Hanmandlu, K.R.MuraliMohan, S.Chakraborty, G.Garg, "Fuzzy modeling based signature verification system", in : Proceedings of the sixth International Conference on Document Analysis and Recognition, USA, 2001, pp.110-114
[5] M.Hanmandlu, K.R.Murali Mohan S. Chakraborty, S.Goel, D.Roy Choudhury, Unconstrained handwritten character recognition based on Fuzzy logic, Pattern Recognition 36 (3) (2003) 603-623.
[6] M.Hanmandlu, K.R. Murali Mohan. Vivek Gupta , Fuzzy Logic based character recognition, Proceedings of the International Conference on Image Processing, Santa Barbara, USA, pp.714-717.
[7] R. Plamondon, S.N SriHari, Online and Offline handwriting recognition:a comprehensive survey, IEEE Trans. Pattern Anal.Mach.Intell.22 (1) (2000)63-84.
[8] C . Quek , R.W.Zhou, Antiforgery: a novel pseudo-outer product based fuzzy neutral network driven. Signature verification system, Pettern Recognition Lett.23 (2002) 1795-1816.
[9] R. Sabourin, R. Plamondon, G. Lorette, Offline identification with handwritten signature images: survey and perspectives, Structured Image Analysis, Springer, New York, pp 219-234, 1992.