

# Identity Theft Mitigation in Kenyan Financial Sectors (SACCOs): Handwritten Signature Verification

Mwangi Caroline Wambui<sup>a\*</sup>, Abade Elisha<sup>b</sup>

<sup>a</sup>*School of Computing and Informatics, P.O. Box 247, Nairobi-00621, Kenya*

<sup>b</sup>*School of Computing and Informatics, P.O.Box 30197, Nairobi-00100, Kenya*

<sup>a</sup>*Email: carolinewmwangi@gmail.com*

<sup>b</sup>*Email: eabade@uonbi.ac.ke*

## Abstract

The existence of identity theft in society has become a major concern due to the effects it causes to those that are affected by it, more especially in the financial sector. Thus this thesis establishes the existence of identity theft issues in the financial sector loan sections and proposes an algorithm that addresses the mitigation processes of identity theft by having the signatures on the loan forms verified using the implementation of the proposed algorithm, then the results are compared with the human experts verification that are done on a daily basis. From the qualitative data collected from the four SACCOs presented indicate the 93% of the respondents knew that forgery of one's signature in the SACCO exists and from the 93%, 95% of them had been victims of identity theft and 50% of them knew it after deductions were made from their accounts. The algorithm was implemented in a prototype that was used to test the signatures that were corrected from various individuals that belonged to various SACCOs. The prototype had successfully verified 80.1% of the test signatures and as expected the highest results from the four Human experts verification of forged signature was 8.3% indicating that they had indicated more signatures as originals. The prototype thus recorded an accuracy of 91.4% and a precision of 60.0%.

**Keywords:** Algorithm; Identity Theft; Mitigation; Handwritten Signature; Signature Verification.

## 1. Introduction

Signature verification is the most common natural way of personal verification.

---

\* Corresponding author.

It is termed as one of biometric aspects in comparison to finger printing and facial recognition. Biometric systems identify individuals based on their distinguishing characteristics [1]. The rise in identity theft in financial institutions that provide loans which require guarantors' authorising signature, gives the need to provide convenient and credible measures when loans are guaranteed in order to draw and maintain customer loyalty. Signature verification is based on two modes; the off-line mode and the on-line mode. In this study we dwell on the off-line mode of signature verification since the SACCO members are given loan forms on which the guarantors would also need to sign on in order to facilitate the loan.

## **2. Forgery**

The art of forgery is as old as the letters of the alphabet. Forgery was practised since ancient times in every country where writing existed and paper was used for financial transaction [2]. Forgeries are classified as follows [3]:

- Random forgery; the forger does not have the shape of the writer signature but comes up with a scribble of his own.
- Unskilled forgery; the forger knows the name of the original signer but not how his/her signature looks like.
- Skilled Forgery; the forger has unrestricted access to genuine signature model, practices it and eventually comes up with a forged sample.

Handwritten Signatures are accepted forms of verification in the process of loan applications. These signatures can be manipulated by forging and using the members' details without their knowledge.

Identity theft dates way back even before the immerging of internet technology or technology in general. But with technology, identity theft has become a common crime and even easier and safer to perform without being caught, thus making it one of the most charted white collar crime [4].

On Identity-Theft-Scenarios.com, [6] Identity theft was once a physical crime. The first criminals who stole identities actually murdered their victims. Once the victim's corpse is disposed, the criminal would then acquire the identity of the victim, ID numbers and other private information [6]. By then, the inspiration was never a real financial gain but it was a way to acquire a new beginning. When the telephone was invented, the identity thieves graduated to using this device to acquire an individual's information like date of birth, addresses, bank accounts since at the end of the call there was a promise of financial rewards or other rewards. Reference [6] This was the first ever gadget that was used in making identity theft easy and it is still used today especially in Africa where we have many who are not informed on the dangers of giving out personal information to someone you do not know about. Then the use of paper shredders was encouraged since people would fish in the trash bins and get thrown away bills or documents that contained personal information [6]. Just as this was thriving, the internet boomed with varying breakthroughs of gathering personal information.

This existing paradigm creates openings for loopholes in information security of both criminal and civil nature

[7]. For instance, identity crime can be achieved in various ways and where an opportunity has presented itself. This may be by assuming your identity to gain employment, gain a loan or open a bank or credit accounts. In this research, the focus is on financial sectors, specifically SACCOs, as institutions through which identity theft has been used to acquire loan/financial credits wrongfully at the expense of the guarantors, institution or agency.

In the world today, the most commonly used means of document authentication of self or another person is a handwritten signature. These documents would be bank cheques, log books, forms like: Opening bank accounts, loan application forms and Visa application forms. All these may either prove what you possess, who you are or what you know. Financial sectors specifically SACCOs offer members loans and make flexible interest percentages of repayment. This has led to forgery of signatures so as to get loans. When acquiring a loan from an existing financial institution, a guarantor's signature is a necessary requirement in the application form, since it is termed as the authentication stamp of the person guaranteeing the loan in-case someone defaulted on payments. This constitutes the falsification of a guarantor's details and signatures. Signatures have their own uniqueness even when forged they can never be an exact of the owner's. Therefore, a research on the key-point features of a handwritten signature on an applicant's form is used and an algorithm that extracts these features is applied thus enabling the verification process of this signature to confirm that the owner of the signature is indeed the one guaranteeing the loan.

In Kenya, so many people have turned to these institutions as a mode of saving and banking since it is easily accessible and can deliver more efficiently to low income earners than the banks. There is difficulty in distinguishing between common fraud which would be the use of someone's credit card or ATM card to conduct financial transaction. The actual act of identity theft takes place when a criminal fiddles with information that directly affects the identity of a person which would be name, address, signature, membership number, date of birth, telephone number, driving licence number among others [4]. This information is then used by the criminal to charade as the victim, gradually taking over his/her identity. With this information, the identity thief may open a bank account, obtain loans, secure employment or even begin a new life in other countries [4].

In one of the SACCOs, a scenario of a forgery case was presented where the one taking the loan applied for a loan and had the guarantors' signatures forged. As the loan was processed, there was no evidence of any existing identity theft. So the client was given his/her loan and for the first few months the SACCO member paid the monthly amount as it was required. Then on the six month the client stopped repaying the loan. At this instance of default, the SACCO gets in touch with the people who had guaranteed the loan and it was at this moment that the guarantors become aware of the particular loan. It was hard for the loan officials to understand how they would not have known about the loan until the loan request form was retrieved and the signatures on the loan forms re-compared to the originals of the guarantors and the mismatch was then detected.

### **3. Identity Theft**

In the current financial environment, the number of SACCO registered and those starting have rapidly increased to bridge the existing gap between the rich and the poor. In any financial environment the economic health is always threatened since there will be someone who will want to make an easy gain. And the use of Identity theft

crime becomes a swift mechanism. Cases of identity theft can be solved if they are discovered earlier or during the build-up of the crime. Thus the research sought to ensure that, in all aspects or undertakings of an institution in Kenya where identity theft is prone to be encountered it is most appropriate to counter attack this beforehand. The research focused on the existence of identity theft in various financial institutions in Kenya.

In identity theft, there exist prominent differences which are determined either by the regions or to a certain percentage according to age. Data available suggests that depending on the form of identity theft, all persons, in spite of social or economic background are potentially vulnerable to identity theft.

The USA Congress in 1998 passed the Identity Theft Assumption and defence Act (the US public law 105-138), stating that an identity thief is anyone who:

*[“Knowingly transfers or uses, without lawful authority, any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.”]*

Thus, identity theft is the thievery of personal information such as a name, date of birth, passport number or credit card information. Any activity in which personal information is shared or made readily accessible to others creates a chance for identity theft to take place.

In identity theft every human being in spite of his/her social or economic background is a potential victim [8]. There are three stages that have been identified which are:

- Acquisition- This is the gaining of information through the web.
- The use of someone’s identity for a financial scam for the benefit of self.
- Discovery- The time taken for full realization of the crime directly relates to the amount lost or gained by a victim [8]. At this stage, the criminal justice system may or may not be involved thus at this point; there is need for extensive research.

Identity theft has been referred to as the crime of the new millennium [9]. The increase in the use of Information Technology facilities like the Internet has led to the rise of crimes and many people are susceptible to various criminal activities. In this study, Identity Theft is considered as a standalone crime reference to the United States as defined in the Identity Theft and Assumption Deterrence Act (1998) and belongs to federal crimes [10].

Identity theft can be accomplished anonymously and easily through a variety of ways as is discussed in the next section. Its experience and consequences to the victims can be shattering. This is readily evident with the recent change of ATM machines and ATM cards [11]. This may also occur through credit or debit (visa) card transactions. Various individuals have gradually discovered transactions in their accounts that they had not authorised from the use of their credit or debit (visa) cards. The identity thief images the information while the customer is knowingly purchasing, then uses the same information to perform malicious activities.

### **3.1. Techniques of Identity Theft**

The techniques employed keep evolving and may vary according to the information corrected from the victim. In this research, the techniques are categorised into various types depending on the various different approaches used to solicit information from an individual.

#### ***3.1.1. Physical Theft Techniques***

This involves theft of sources of personal information: Any item that stores data like a cell phone, iPad or any item which may carry important documents like a wallet and a purse. Then there is dumpster diving, where identity thieves will trash ones household garbage, business trash in order to pick up any paper bills or pieces of paper which may be containing the information they require. The most important thing for this technique is for a company or even at home to ensure that the paper disposed is either shredded or disposed in a way that one cannot pick it up and gain important information. Like in Kenya this would be the ATM slips, copies of one ID or passport and so on.

Change of address and mail theft is also used to get the necessary information. When the identity thieves target ones mail, they will redirect it to another address to which it will go to. This has proved sufficient mostly in the US and Canada where there have been cases of this nature. Through mail redirect, the identity thief gets the necessary information the easiest way possible and abundant time to commit the crime before the victims can even make sense of what is already taking place. Mail theft is easily achieved by getting it from the mail boxes and recycling bins. For instance in Kenya, people still share post boxes making it a very easy technique from which one can acquire the necessary information.

Another technique is where a company engages a person in what seems as a legitimate business. This may be through wire transfers in an auction or a reshipping deal of some items. This scheme becomes a way of acquiring one's personal information, credit card and auction fraud. The victim is usually contacted through chat rooms, over the internet or bulletin boards for job applications.

In the process of digitization, governments are making public records accessible online through other electronic means. While their aim is to reduce costs, make service more readily available and boost openness and accountability, it has significantly become a benefit to identity thieves who gain access to personal information and defraud unsuspecting individuals.

There are also cases where personal information of a deceased person can be accessed from newspapers. This is generally referred to as Tombstone theft. Obituaries mostly provide a person's full name and date of birth. Uninformed funeral homes may also pass out information. All this enables the identity thief to acquire loans or even withdraw from their account like a case in Atlanta, where 80 deceased persons' information was sold for \$600 each and then used to acquire car loan totalling to \$1.5 million [5].

Skimming and personal information trafficking is another means characterised under the techniques of physical identity theft. Skimming is not only limited to debit, credit and calling cards since there are so many other cards

that are now in existence and use magnetic strips to store information. For example airline boarding passes contain loads of information on an individual as indicated on the Guardian Unlimited. Personal information trafficking is achieved by “Carder Networks” and other underground networks. The information available in these sources will be as a result of insider abuse or remote exploitations of computer vulnerabilities to access clients databases [5].

An insider job is also a major contributing factor to how one’s personal information gets into the wrong hands. The security of the information is only as good as the integrity of the employees. Once the identity thief has some information he would need to dig deeper to acquire more sufficient information this is known as identity consolidation or “identity breeding”. For example if an identity thief has someone’s ID, he or she can use this to get a sim card replacement then use this sim card to siphon money from unsuspecting persons by calling them, requesting for information to offer rewards, job promises as long as they get some money from the victim, sending false M-Pesa messages and luring the receiver to send back the money when there was nothing sent.

### ***3.1.2. Technology-based Techniques***

Phishing is a technique that involves the use of a social engineering by camouflaging as a trustworthy organization in an e-mail message or through their web platforms [12]. Email messages become the main channels of gathering the necessary information from the victims. The phishing messages have become very sophisticated that it is very hard to determine their legitimacy. They may appear as if they have been sent from a bank, indicating an issue with your account that would need immediate attention. These messages are written with a somewhat similar message as the organization would use and the identity thieves also ensure that colours and logos are of the same brand. This is known as spoofing [12].

Spoofed websites are used to entice victims who are then manipulated to accomplish the Phishing technique [13]. This can be accomplished in two ways, mapping legitimate domain names to legitimate IP addresses with the aim of compromising computer host files and Domain name system poisoning. Exploitation of the DNS is done so as to gain control of the existing website and change the numerical address associated with the textual domain name. This results to any victims visiting the actual address been referred to the spoofed site, but the address bar on the victims browser never changes from the obvious. This is also similar to DNS Cache Poisoning whereby the addressed is changed locally on the actual machine accessing the website instead of the DNS server.

The other technology-based technique applied is the Spyware programs [14]. They are known for slowing down or even crashing the system and may also cause unwanted advertising and perpetual pop-up messages. This may seem unimportant but in the unknown the spyware tracks the activities of the computer user or enable access to the content of the hard-disk drive. This is because the spyware programmes are able to send information via the internet to the creator of the spyware [14]. It usually consists of the core functionality which appeals to users and entices them to install and use the spyware and functionality for information gathering.

Internet searches and Google hacking can also be a great source of information [15]. Searches from legitimate websites could give vital information of employees or management members. Google hacking consists of using

Google search engine to find “hidden” documents on a website [15]. Many organization have no idea just how much information one can get from their site if it is not properly managed and configured. This would include payroll details, contacts, ID numbers, NHIF details among others. Apart from Google hacking the other type of hacking that can be used involves exploiting known security holes and vulnerabilities in softwares such as Microsoft Windows [15]. For this to take effect corrupt data and a set of instructions are sent to the softwares running on a targeted computer. The corrupted data confuses the software and it start executing the new instructions sent by the hacker. Also, information for a large group of people can be captured by hacking into and stealing data from financial or government databases of business. For example In China, there exists lack of individual privacy concerns and mechanisms for public protection thus making it a potential ground for identity theft [16].

With the rise of wireless technology, many home users are now getting connected. Identity thieves will visit neighbourhoods detecting these Wi-Fi wireless networks. Wireless equipped laptops, PDAs and other softwares are used to detect the unsecured wireless networks. Once a connection is established then the identity thief can go ahead and acquire the information he/she needs from the device.

When organizations are doing an upgrade of their servers or PCs or a home owner needs to sell out an old PC, they will just sell the out or sometime donate them to schools and so on. The hard-disk drive may have “mother lodes” of the former owner. For servers if they had been used to store up the organizations database, then it would have this information that would be retrieved from it. So when discarding this devices proper measures should be taken since just deleting them from plain site does not necessary mean the using the computer forensics softwares of data recovery or the other existing softwares that are commonly used for data recovery cannot be applied to reveal the still present that is locked away on the hard-disk drive [17]. Students in a Massachusetts Institute of Technology proved that wrongly disposed computers equipment posed high risks. They purchased used computer hard drives and then scanned them for personal information. They recovered medical e-mails that contained personal information and credit card numbers and so much more, thus proving the gold-mine in improperly disposed of computer equipment.

### ***3.1.3. Social Engineering Techniques***

This involves the natural aspects of a person in trusting someone else especially those that are close to them. Remarkable efforts have been made in the past years by governments, business and academic research community in understanding the Identity theft issues and also developing solutions to deal with the crime from a social, technological, law enforcement and legislative, business and management angles [16].

One of the most effective ways of achieving identity theft is through “Social engineering”, it involves: An Identity theft criminal contacting the victim directly and convincing them to disclose passwords or other information by posing as agents representing an organisation or a particular individual [16]. This is a common aspect in Kenya. We have had public notices made on the newspapers concerning employees who have left an organisation [18]. The victims can also be targeted via the internet by the use of social engineering like the use of email messages, phone text messages, or intercepting and capturing financial or identity information while transaction is in progress. This trust can be exploited by identity thieves through various ways as indicated in

this section to acquire the information they need [5]:

- Pre-texting: This involves “smooth talking” the victim into trusting you and eventually persuading them to give off vital information
- Obtaining credit reports: Identity thieves may pose as legitimate business people such as landlords, potential employer and used car dealers but with the interest of getting their credit reports.
- Bogus Employment and Visa Processing Schemes: This is the most common way identity thieves use to get ones information especially in Kenya. Instances of people complaining on the assurance given when filling forms and copies of their documents they had given out only for the said to just vanish and the person completely dupes them and robs their personal information and some amount of cash too.
- Through Contests and Surveys: unwitting victims may give off personal information while under the impression that they are joining up a contest or participating in surveys. This can happen through written submissions to contents or draws for prizes.

#### **4. Methodology**

The research design entails the chosen life cycle of the research in which it shall run, the data collection methods outlines the best of the existing methods that shall be used to gather the required information for the success of this research and the analysis method/tools that are applied to analyse the collected information. Finally validation of the data is established.

##### **4.1. Research Design**

For this study, the qualitative research design has been applied to enable the collection of data facts and explaining of the phenomena more deeply and exhaustively. The study critically examines the knowledge of Identity theft among Kenyan Citizens and investigates the existing logical processes that are stipulated in the constitution for Identity theft reconstruction purposes.

Qualitative research design sequence and methods have been applied in the research are: Assessment of a problem statement, formulation of research questions, selection of a population sample, collection of data and analysis and lastly but not least, the presentation of the findings and conclusions [19].

This research design also entails giving empowerment to the persons been evaluated by having question that allow them to give their own opinions and voice out their ideologies or concern on the topic of discussion. This assures the respondents, thus making them more willing to participate in the undertakings. It also enriches the data collected making conclusions made unbiased and full informative thus producing almost accurate outcomes in the data analysis processes.

For the algorithm design, the Constraint Satisfaction Problems technique of developing an algorithm was implemented since the algorithm works with random generated keypoints from the scanned image. In Constraint Satisfaction Problems technique, the constraints are the key component in expressing a problem and are determined by the way the variables and the set of values are chosen [20]. Constraints are a logical relation



among a set of variables [21] and they limit probable values that variables can obtain for example [20] all-different(X1, X2, X3). This constraint says that X1 X2 and X3 should acquire differing values thus with a set of values {1,2,3} created for each of the set should be X1=1, X2=2 and X3=3 [20]. It also symbolizes some partial information regarding the variables of interest [21]. The Constraint Satisfaction Problems technique involves 3 components [20] and [21].

- A set of variables: Randomly generated keypoint variables from the scanned image
- A set of values for each of the variables
- A set of constraint restring the values between various collections of variables

An assignment of a value from its set to every variable satisfies all of the constraints. Constraint propagation enables forward checking which controls the future conflicts from the value set formed and enables earlier pruning as shown in fig. 1 [21].

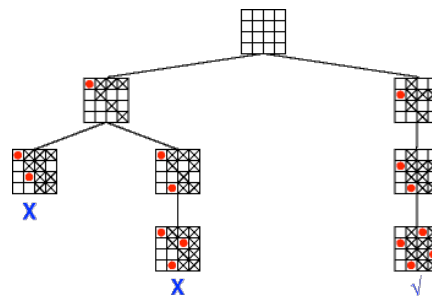


Figure 1: Constraint Propagation

#### 4.2. Research Setting

The proposed County of research is Nairobi County.

#### 4.3. Study Population

The population under study shall involve the members of four participating SACCOs and the staff members in these SACCOs as well.

#### 4.4. Sampling

In this research, the data gathering process was guided by a sample of persons from various SACCOs. Convenience sampling provides the most convenient and cost effective method of selecting the study group [22]. This is because it eases the cost of locating elements of the population, the geographical distribution of the sample and obtaining the data from selected elements [22]. It involved visiting SACCO offices or SACCO AGM meetings for those that agreed to participate in this research to seek participation of the individuals in this SACCOs. This ensured that the target sample of research is only members of a particular SACCOs. With this information a hypothesis was established on the knowledge and actions taken on identity theft in SACCOs.

#### 4.5 Data Collection Method

Since this research is more societal based the experimental research best applied. This helped in the testing of the effectiveness of the prototype that that was developed from this research and how efficient it proved in dealing with identity theft crimes. The experimental research provides a method of investigation to derive basic relationships among phenomena under controlled conditions or to identify the conditions underlying the occurrence of a given phenomenon [23].

#### 4.6 Research Evaluation

In this phase the Evaluation method was be applied so as to enable the measure of the True positives against the False positives and True Negatives against the False Negatives [24]. The true positives (TP) shows the number of negatives identified and true negatives (TN) are correct classifications. A false positive (FP) is when the outcome is incorrectly predicted as yes (or positive) when it is actually no (negative). A false negative (FN) is when the outcome is incorrectly predicted as a negative when it is actually positive [24]. Thus, the TP is where the signature accessed, is the original signature of the writer while the FP is the forged signature of a writer but it is viewed as an original due to the similarities in the stroke aspects of the signature. The TN is where the forged signature is identified through the algorithm verification procedure while the FN is where an original signature of a writer is termed as a forgery yet it is his/her actual signature and this is summarised in the figure below [24].

**Table 1:** Evaluation Matrix

Actual Condition (Truth)			
(-ve) Forgery	(+ve) Geniune		
<b>FP</b>	<b>TP</b>	(+ve) Geniune	Output of the system
<b>TN</b>	<b>FN</b>	(-ve) Forgery	

The Original Signature rate (Sensitivity):

$$\left[ \frac{TP}{TP+FN} \right] 100\%$$

The Forged Signature rate (Specifity):

$$\left[ \frac{TN}{FP+TN} \right] 100\%$$

Accuracy:

$$\left[ \frac{TP + TN}{TP + TN} \right] 100\% \quad (1)$$

$$TP+TN+FP+FN$$

Precision: (2)

$$\left[ \frac{TP}{TP+FP} \right] 100\%$$

#### 4.7. Research Validation

Validity is largely determined by the presence or absence of systematic error in data [19]. In this case, we shall be justifying the results gathered and how effective they are to the new acquired information. The gathered data was theorised in the aim of confirming the gathered information, thus making it a continuing process of building assurance in the effectiveness of the acquired information.

#### 4.8. Data Analysis

Collected data was cleaned in order to determine incomplete, or unreasonable data and then improve the quality through correction of detected errors and omissions. Then data was entered for analysis using the Microsoft Excel package.

#### 4.9. Human Expert Comparison

Since the SACCOs' have loan officers who offer the loans to various individuals, it is necessary to compare the way in which this loan offices verify signature and the way in which the system will perform the same duty. Thus the experiment involved the participation of four loan officers each examining the signatures used in the system as well.

#### 5. General Procedure

Design is concerned with establishing how to deliver the functionality that was specified in analysis while, at the same time, meeting non-functional requirements that may sometimes conflict with each other (Simon & Ray, 2002). It is the gaps found in the literature review that motivates the design of a prototype for Signature verification. The particular aspect that this research addressed is the fraud that occurs as people seek to acquire a loan and guarantorship is the main security of the loan. Fig. 2 below shows a Loan Management system that requires a guarantor for loan applications. The algorithm proposed closes this gap by ensuring that the guarantors' details are clearly confirmed in order to erase any unfriendly activity. An offline option was chosen for the system since the forms are still filled on paper thus making it quite efficient.

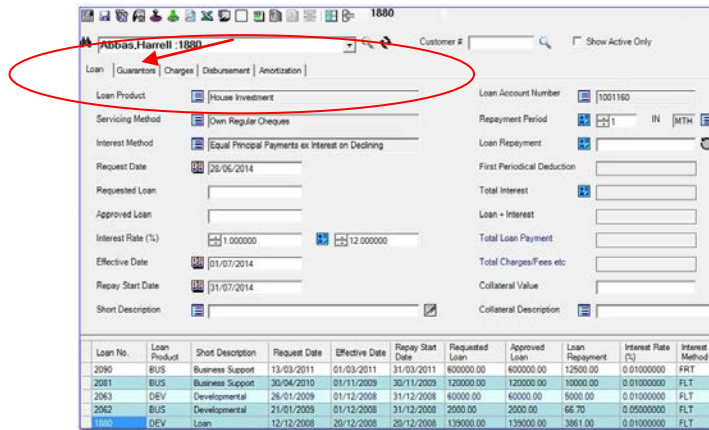


Figure 2: Loan Management system

### 5.1 Image Matching Process

There exists different images that are to be processed and values attained. Thus the following matching process is used as established in the figure 3 below [25].

### 5.2 Vector Rasterization

The image is described in vector graphics form thus in this stage it is changed to a raster form so that it is read as a bitmap file format.

### 5.3 Ascertain the Reference Object

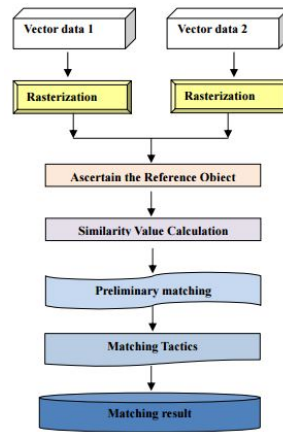
The image inputs are referenced to check for the critical points required to do a similarity value calculation.

### 5.4 Similarity Value Calculation

The Euler number calculation is adopted so as to establish values of the objects which have been identified during the ascertain the reference object stage.

### 5.6 Preliminary Matching

If the similarity values of the objects are within the scope of threshold, the preliminary conclusion are thus established which will imply that the images are homograph entities.



**Figure 3:** Matching Process

**5.7. Proposed Algorithm**

The algorithm works for both the database image and the scanned image. This is because features are extracted from both images (173x116 px) and then analysed and matched. The algorithm can be summarized as follows:

- Signature feature extraction: Key point, these points are extracted by scanning the image for pixel continuous forming a line or a curve, from the scanned image and database image and from this, the Critical points are created.
- Critical points are selected within a rectangular space. From this area a random selection of points is done where the signature has unique characteristics. This can be a corner or a full-stop depending on how your signature appears.
- From the vectors collected in the plots of the two images X1 and X2 {a1,a2, a3, a4, a5, a6, a7, a8, a9...an} and {b1, b2, b3, b4, b5, b6, b7, b8, b9...bn} a two dimensional matrix is created from it. (a1,a2, a3, a4) and (a5, a6, a7, a8).
- Matching of the signature [26], SCE based matching using the Directional Difference Matching (DDM). Construction of the comparison matrix is done with its components as binary numbers. The matrix comparison of input SCE from the scanned image and SCE from the database image is done. The following equation for comparison is applied [26]:

$$[X1, X2]= Y+ \epsilon$$

- Y in this instance represents the Euler number/Difference from input Euler code and  $\epsilon$  is the tolerant error. The value of X lies between X1 and X2 then it is indicated as 1 in the comparison matrix otherwise a 0 is adopted. To match the signatures, the numbers of 1's and 0's in the matrix are counted. The 1's refer to a match while the 0's refer to a mismatch.

**6. Results**

The results shall be made in comparison with the human expertise on signature verification. A total of 532

signatures were used. 66 of which were database signatures and while 466 signatures were test signatures. For each class of know signatures contained both a training and a test signature. The overall performance of the signature verification process was measured in terms of accuracy in which it would determine the genuine or forged signature in a particular test.

Figure 4 and Figure 5 below are original signatures from two members with member number 3001 and 3005 respectively from the database.






**Figure 4:** Member no 3001's Signature      **Figure 1:** Member no 3005's Signature

**6.1. Experiment results**

In this section a sample of the tested signatures are presented. Signatures from the same known writer were tested against each other as shown in Table 2 below. The critical points picked had a threshold that did not exceed the set value. Then in Table 3, an unknown signature was used to be tested. It was classified as a forgery signature as the results are shown below. From this experiment the test signature used can be classified as a skilled forgery coz from a glance one would say it may be one and the same as the owners.


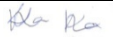
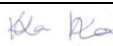
**Table 2:** Point variants of known signatures

Signatures	Critical Points	Time (Nano)	Verification
 13.jpg   14.jpg	Set1(12,13)	1678	Signatures match
 13.jpg   15.jpg	Set2(12,12)	1666	Signatures match
 14.jpg   15.jpg	Set3(13,12)	1550	Signatures match







The next experiment shows signatures in table 4 which are from the same know writer. And as in the experiment above we test them to verify them against each other. Then in Table 5 the known signatures in Table 4 were

tested against an unknown signature and from the results it was determined as a forgery.

**Table 3:** Point variants of test signature 16.jpg and known signatures

Signatures	Critical Points	Time (Nano)	Verification
 13.jpg   16.jpg	Set1(12,24)	1389	Signature Mismatch
 14.jpg   16.jpg	Set2(13,25)	1354	Signature Mismatch
 15.jpg   16.jpg	Set3(14,25)	1411	Signature Mismatch

**Table 4:** Point variants of known signatures

Signatures	Critical Points	Time (Nano)	Verification
  21.jpg   23.jpg	Set1(29,30)	1469	Signature Match
  22.jpg   23.jpg	Set2(28,30)	1472	Signature Match
  21.jpg   22.jpg	Set3(29,28)	1464	Signature Match

## 6.2. Discussion of results


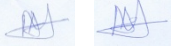

In this section the proposed evaluation techniques of the signature verification are applied.

The matrix on the true positive, true negative, false positive and false negative is established in order to establish the preciseness at which the forged signatures are determined.

Out of the 532 signatures the prototype achieved the following results: The percentage of accuracy in this test

was 91.4% while the percentage of precision was 60.0%.

**Table 5:** Point variants of test signature 24.jpg and known signatures

Signatures	Critical Points	Time (Nano)	Verification
 21.jpg   24.jpg	Set1(29,44)	1264	Signature Mismatch
 22.jpg   24.jpg	Set2(28,44)	1260	Signature Mismatch
 23.jpg   24.jpg	Set3(30,44)	1262	Signature Mismatch

**Table 2:** Results from Prototype

TP	11.3%	FP	7.5%
TN	80.1%	FN	1.1%

There were 66 members that were recorded in the database and each member was asked to provide ten of her/his signatures. Thus in total there were 66 original signatures that were recorded in the database which thus were termed as the actual member's signature.

Then as earlier stated 532 signatures were used as the test and training signatures. Out of these signatures 80.1% of the signatures were clearly identified as forgeries while 7.5% out of the test signatures were identified as originals, marking them as skilled forgeries.

From this test it indicated that signature may vary depending on the pen used, circumstance while signing and so on.

### 6.3. Comparison with Human Expert

The human experts from four different SACCOs were asked to have a look at the sets of signatures and compare them to the Original signatures.

They were shown the original signatures, then they were to compare with the 532 test signatures. The results are as presented in the table below:

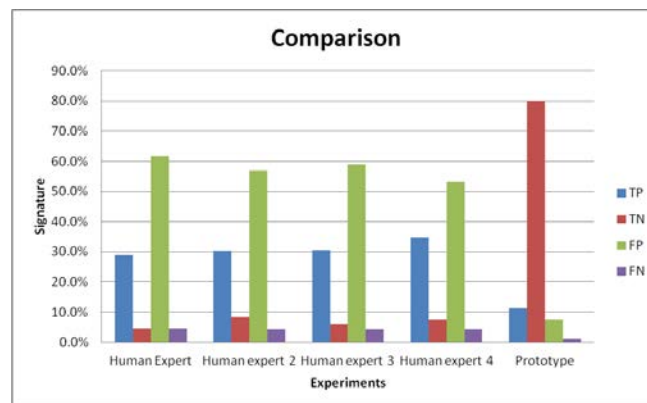


**Table 7: Results from Human Expert**

Human Expert	TP	TN	FP	FN
1	28.9%	4.7%	61.7%	4.7%
2	30.3%	8.3%	56.9%	4.5%
3	30.6%	6.0%	59.0%	4.3%
4	34.6%	7.7%	53.2%	4.5%

As this experiment with the human experts was conducted some factors were indicated as situations at which one may not even check the signature as long as the guarantor is a member and there is an imprint at the signature section also the fact that we are human there may be something that is over looked in the process. In comparison to the results the signatures verified by the human eye had few forgeries while in really sense the test signatures totalled to 466 signatures. While the other 66 signatures where the copies of the same signatures in the database.

Thus from the results above the human experts indicated a very high percentage e.g. human expert1 had 61.7% of the false positive signatures (forgeries termed as originals) and a low on the true negatives (forgeries) e.g. human expert 1 had 4.7% while has indicated by the prototype above the vice versa should have been the case. Thus the percentage comparison of the human experts and the results from the prototype were as follows:

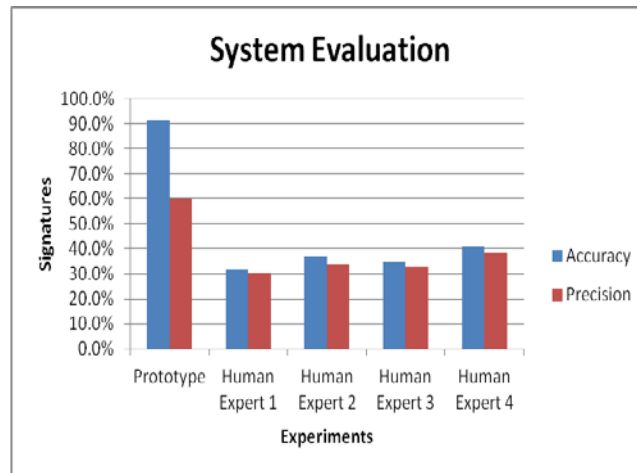


**Figure 6: Comparison**

#### 6.4. Evaluation of the system

Evaluation of the system performance was done through statistical analysis of experimented results and compared to the human expert experiment.

Statistical results in terms of accuracy (1) and precision (2) were calculated.



**Figure 7:** System Evaluation

**6.4.1. False Acceptance Ratio**

This is the evaluation of the probability that the system may erroneously accept a forged signature as an original signature. (3) It is calculated by dividing the number of false signature acceptances (FP) by the number of total Test signatures [27].

$$\left[ \frac{\text{FP}}{\text{Total test signatures}} \right] \times 100 \quad (3)$$

Thus making the percentage FAR of the system 7.5%

**6.4.2. False Rejection Ratio**

This is the evaluation of the probability that the system may erroneously reject the original signatures and mark them as forged signatures. (4) It is calculated by dividing the number of false rejections (FN) by number of identified know original signatures [27].

$$\left[ \frac{\text{FN}}{\text{Total No. of Known Original signature}} \right] \times 100 \quad (4)$$

Thus making the percentage FRR of the system 9.1%

For a good working system it should have a low FAR and a high FRR which would thus ensure that no

unauthorized transactions are allowed [27]. This also implies that some several tests would need to be redone.

## **7. Conclusion**

The general objective of this project was to analyse features on a signature that are imprinted on loan forms by the guarantors and propose an algorithm and develop a prototype that will enable the verification of this signatures and thus enhance efficiency in the handling of the identity theft cases. The algorithm proposed used the Euler number as the mode of attaining the keypoints from the 2d image of the signature that are retrieved from the database and scanned from the forms. The evaluation of the identity tactics and establishment of red flags was conducted through the filling of questionnaires and this helped in actualising the projects necessity. From the project Signature verification with the application of the algorithm was termed more accurate and timely unlike when conducted by a human expert as shown in the results above. The human expert eye will seek to outline the most visible set of strokes that may seem to look similar in one way or the other while for the system it looks at wholes found in the image pixels and use this to determine the signatures validity. Due to the pressure one uses to imprint their signature on a paper the ink placement largely varies.

### **7.1. Comparison with other existing Applications**

Signature verification algorithm was based on static and dynamic features of online signature data [26]. The texture and topological features are extracted from the signature image while a digital table captures in real-time the pressure values, breakpoints and the time taken to create a signature [26]. Euler numbers were used to analyze the textural and topological features of the signature [26]. With this application they system had an accuracy of 98.18%. Classification of offline handwritten signature using wavelets and a pattern recognition neural network [28]. Their system implemented Discrete Daubechies Wavelet transform to extract wavelet coefficients in three directions namely horizontal, vertical, diagonal and a pattern recognition neural network classifier is designed where the training algorithm is a Quasi-Newton algorithm and the classification is done [28]. Their system had a false acceptance rate quite high, and indicated that some modifications in the form of increasing the number of hidden layers and their nodes along with the more efficient training algorithms are highly desirable and have the potential of better accuracies [28]. Anand et al [29] enhanced signature verification and recognition using Matlab. They indicate feature extraction as a main necessity for successful results in a system. They implement neural network for the verification of signatures. Various features are used in the creation of the features set used in the proposed system, eccentricity, skewness, solidity, entropy, Euler number just but to mention a few. For this project Euler number application to acquire the features from the scanned signature images was applied and a handwriting analysis done for the line or curve in the images that was then compared to the data collected from the images of the known signatures stored in the database. Its accuracy been at 91.4% and precision at 60.0%.

### **7.2. Contribution to Previous Work**

Previous studies of use of signature verification like Jarad et al [30] offline handwritten signature verification system using a supervised neural network approach aims at limiting the computer singularity in deciding

whether the signatures are forged or not but in turn allows the signature verification personnel to participate in the decision making process through adding a label which indicates the amount of similarity between the signatures that are been analysed [30]. While other works suggested the use of Associative Memory Net [31] and Contourlet transform [32].

This research proposes an image based verification application that implements the measure of the boundary from which a point is calculated and plotted on the image then a rectangle plotting done from each pixel values are vectorised and then a matrix which gathers points from these vectors is developed in order to aid in the comparison using matrix comparison methods.

### **7.3. Limitations**

- The openness of the financial sectors on how they manage their information.
- From exiting financial sectors, Savings and Credit Co-operatives (SACCOs) were more readily accessible and willing to offer information that would help in driving the research forward. Thus the research covered only a fraction of the existing financial sectors in Kenya.
- Time limitation on conducting a full research on the known identity theft cases in more financial institutions other than SACCOs
- The recognition of Identity theft as a crime in the institutions' constitution and how to deal with it.
- The changing nature of the identity theft crime and the fact that it is still concealed.

### **7.4. Further Research**

This research focused on the offline version of input since the forms are still filled manually. An online version of the system can be created in which one can sign on a tablet and the signed signature is registered and verified real time through the online process. If the manual form is not altered the scanning of the signatures on the forms can be made easier by having it done via a scanning mobile application. For the algorithm, since the image is a scan at times it may appear dirty, crumbled or blurry depending on the scan done, thus a rasterization may be necessary in order to map it from picture geometry and onto pixels this could not entail much since the algorithm applied and does not impose a specific way to work out the colour of those pixels and neither would rasterization require one to do so.

### **Acknowledgements**

I appreciate the support I received from the staff and members of all participating SACCOs in this research.

### **References**

- [1]. Zimmerman Thomas G. , Russell Gregory F. , Heilper Andre , Smith Barton A. , Hu Jianying , Markman Dmitry , Graham Jon E. , Drews Clemen, "Retail Applications of Signature Verification, Almaden: IBM Research", *IBM Almaden Research Center*, 2003.
- [2]. Koppenhaver, K. M., "History of Forgery, Forensic Document examination", Humana Press, 2007.

- [3]. Karounia, A., Dayab, B. & Bahlakb, S., "Offline signature recognition using neural networks approach." *Elsevier Ltd, Procedia Computer Science*, 2011, Volume 3, pp. 155-161.
- [4]. CIPPIC, "Identity Theft: Introduction and Background", *Ottawa: CIPPIC Working Paper*, 2007, No. 1.
- [5]. CIPPIC, "Techniques of Identity Theft", *Ottawa: CIPPIC Working Paper*, 2007, No.2.
- [6]. Identity-Theft-Scenarios.com, "History of identity Theft", 2015, Available online: <http://www.identity-theft-scenarios.com/identity-theft-facts/history/>
- [7]. Barske, D., Stander, A. & Jordaan, J., "A Digital Forensic Readiness framework for South African SME's", *Information Security for South Africa (ISSA)*, 2010, (DOI) 10.1109(ISSA.2010.5588281).
- [8]. Graeme, N. R. & McNally, M. M., "Identity theft Literature Review" *U.S. Department of Justice*, Report 2005.
- [9]. Hoar, S. B., "Identity Theft: The Crime of the new Millennium", *HeinOnline journals*, 2001, pp-1423(80).
- [10]. Ogla, A., "ID Theft: A Computer Forensics' Investigation Framework. Australia", *5th Australian Digital Forensics Conference Paper*, 2007.
- [11]. Maxwell, M., "Police warn over card skimming syndicate, Nairobi" *Star newspaper*, 2012.
- [12]. Oppliger, Rolf and Gajek, Sebastian. "Effective Protection Against Phishing and Web Spoofing", *IFIP International Federation for Information Processing*, 2005, pp. 32-41.
- [13]. Vishesh, T., "Phishing and Pharming- The Deadly Duo" *SANS Institute*, 2007.
- [14]. Post, A., "The Dangers of Spyware", *Symantec Security Response*, 2003.
- [15]. Billig, Justin, Danilchenko, Yuri and Frank, Charles E., "Evaluation of Google Hacking" *Kennesaw InfoSecCD Conference '08*, 2008.
- [16]. Shao-Bo, J., Shawn, S.-C. & Quing-Fei, M., "Systems Plan for Combating Identity Theft- A Theoretical Framework", *Journal of Service Science and management*, 2008, Volume 1, pp. 143-152.
- [17]. SecurityFocus, "Discarded computer hard drives prove a trove of personal info", *Security Focus*, 2003. Available online: <http://www.securityfocus.com/news/2055>
- [18]. 22nd September Monday, *DailyNation*, 2014. Public Notice Adverts. Nairobi: Monday Daily Nation.
- [19]. Mugenda, O. M. & Mugenda, A. G., "Research Methods: Quantitative and Qualitative Approaches", Second edition *Acts Press*, 1999.
- [20]. Bacchus, F., Computer Lecture notes, 2010, [Online] Available at: <http://www.cs.toronto.edu/~fbacchus/Presentations/CSP-BasicIntro.pdf> [Accessed 16 July 2015].
- [21]. Wagner, M. & Urli, T., 2013. Computer Lecture notes. [Online] [Accessed 16 July 2015].
- [22]. Battaglia, M. P., "Nonprobability Smampling. In: Encyclopedia of survey Research methods", *SAGE Publications*, 2008, pp. 523-526.
- [23]. Ross, S. M. & Morrison, G. R., "Experimental Research Methods", *Association Educational Communication and technology*, 2001.
- [24]. Witten, I. H., Frank, E. & Hall, M. A., "Data Mining Practical machine Learning Tools and

- Techniques” 2011, *Morgan Kaufmann Publishers*, 3rd ed.
- [25]. Li, G., Zhiping, L., Bin, Z. & Yaoge, W., “The study for Matching Algorithms and Matching Tactics about area Vector Data Based on Spatial Directional Similarity” *The Joint International Conference on Theory, Data Handling and Modelling in GeoSpatial Information Science*, 2010, 38(II), p. 395.
- [26]. Vatsa M., S. R. M. P. N. A., “Signature Verification Using static and Dynamic Features” *Berlin Heidelberg: Springer-Verlag*, 2004, pp. 350-355.
- [27]. Thakkar, D., “Bayometric: False Acceptance Rate (FAR) and False Recognition Rate (FRR)”, 2016, Available online: <https://www.bayometric.com/false-acceptance-rate-far-false-recognition-rate-frr/>
- [28]. Patil, P. G. & Hegadi, R. S., “Classification of offline Handwritten Signatures using Wavelets and a Pattern Recognition Neural Network” *International journal of Computer Applications, Recent Advances in Information Technology*, 2014, pp. 0975-8887.
- [29]. Anand, H. & D.L, B., “Enhanced signature verification and recognition using Matlab” *International Journal of Innovative research in Advanced Engineering (IJIRAE)*, 2014, 1(4), pp. 2349-2163.
- [30]. Jarad, M., Al-Najdawi, N. & Tedmori, S., “Offline handwritten signature Verification System using a Supervised Neural Network approach”, *IEEE Computer Society*, 2014, pp. 189-195, 6(ISBN:987-1-4799-3999-2)
- [31]. Dash, T., Nayak, T. & Chattopadhyay, S., “Offline Handwritten Signature Verification using Associative Memory Net”, *International Journal of Advanced Research in computer Engineering & Technology*, 2012, vol. 1(4).
- [32]. Pourshahabi Muhammad R., Sigari Mohamad H. and Pourreza Hamid R., “Offline Handwritten signature identification and verification using contourlet transform”, *IEEE Computer Society*, 2009, Vol. 2, pp. 670-673.