Secure Rural Supply Chain Management Using Low Cost Paper Watermarking

Ashlesh Sharma
Department of Computer Science
New York University
New York 10012
ashlesh@cs.nyu.edu

Lakshminarayanan Subramanian
Department of Computer Science
New York University
New York 10012
lakshmi@cs.nyu.edu

Eric A. Brewer
Department of Computer Science
University of California, Berkeley
California 94720
brewer@cs.berkeley.edu

ABSTRACT

Supply chain systems in rural developing regions are extremely fragile and are vulnerable to a wide range of security threats including theft, fraud and counterfeit goods. In this paper, we propose the design of a secure, low cost supply chain management system that leverages cheap cellphones and a low-cost paper watermarking system that can authenticate and verify the integrity of goods in a supply chain. Unlike many sophisticated solutions which have deployment problems due to the harsh ground realities in rural regions, our system is easy to use, deploy and does not require significant changes to the existing operational model. In addition, our system relies only on paper and cellphones, both of which are ubiquitously used in rural developing regions.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection
; I.4.1 [**Computing Methodologies**]: Digitization and Image capture—*Document Capture*

General Terms

Design, Security, Experimentation

Keywords

supply chain, paper authentication, paper speckle

1. INTRODUCTION

Theft and fraud in supply chain management systems are major problems in developing regions especially in rural areas. In the last few years, several such incidents have been reported resulting in significant monetary losses [3, 1]. For example, the supply of ARV drugs at subsidized rates by pharmaceutical industries to combat AIDS in Africa has resulted in billions of dollars loss due to parallel trading and counterfeit
drugs[3, 1].

In rural regions, almost all local businesses and organizations including banks, agricultural societies, pharmaceutical industries and microfinance institutions are completely dependent on a supply chain backend to provide several essential services. However, given the completely ad-hoc nature of functioning in rural areas, supply chain systems do not have any basic form of accountability thereby making them susceptible to theft, fraud or counterfeit goods.

In this paper, we investigate the problem of *developing a low-cost and deployable solution that can aid in securing rural supply chain systems.* Unfortunately, there is very little work in this space and the harsh ground realities also make it exceedingly difficult to deploy any form of sophisticated security solutions [13, 22]. First, most transactions in supply chain systems especially in semi-urban areas are paper-based with very little electronic automation. Paper is inexpensive, portable and extremely simple to use; hence, paper is ubiquitously used as the primary medium for identification, authentication and recording important information. Second, in most regions, using a PC is often a luxury and most people may not have the expertise to operate them.

In such settings, for any security solution to be practical and adoptable, it is essential for the system to be low-cost and not require significant changes to the current model of supply chain operation. In a survey conducted by CGAP [19], PDAs used in microfinance transactions by SKS Microfinance and Compartamos proved to be too expensive [19] due to their high hardware and software costs. Point of Sale (POS) devices that are being used in Africa by several microfinance institutions backed by Hewlett Packard [19, 6] are not flexible for different business processes and difficult to blend with the existing backend of organizations [16, 8]. Hence, to ease deployability, it would be best if the security solution were to inter-operate with the existing functioning of these supply chain systems.

In this paper, we propose the design of a cellphone and paper based, secure, low cost supply chain management system that caters to the businesses of rural developing regions. In our design, we leverage our earlier work on *PaperSpeckle* [20], a low-cost tamper-resistant paper watermarking system that uniquely identifies any piece of paper. *PaperSpeckle* is highly appropriate for developing country settings since, it primar-

NSDR'08, August 18, 2008, Seattle, Washington, USA.

ily relies on a microscope for authentication. *PaperSpeckle* is also significantly cheaper than prior paper watermarking techniques [23, 21, 4]. We have tested *PaperSpeckle* and shown that it is robust and tamper-resistant in the wake of extreme modifications to the paper such as crumpling, soaking in water and aging.

The key idea in our approach is to use *PaperSpeckle* to generate unique watermarks of paper-based transactions and use cellphones to disseminate these signatures and remotely verify the correctness of these watermarks. The motivation to use cellphones to disseminate and verify watermarks are three-fold. First, most rural regions in the developing world in Asia, Africa and South America have good cellphone coverage. Many countries in Africa such as Ghana and Rwanda have more than 60% cellphone coverage [2]. Second, the cost of cellphones have significantly reduced in these regions and cellphones are readily available; in the shared usage model, it is common for users who cannot afford cellphones to own SIM cards but share a common cellphone. Third, rural users are fairly comfortable with the cellphone interface making it a user-friendly device.

Our system offers strong security guarantees in terms of tracking the flow of goods in a supply chain environment. If a good where to traverse several different service points between a source and a destination, our system can provide a way of tracking the good through every stage of the supply chain. While it cannot prevent theft of goods, it can definitely aid in identifying the potential sources of theft in the system. The hope is that being able to pinpoint the source of theft would act as a sufficient deterrent to reduce theft and fraud. Overall, our system offers several benefits: *low-cost, portable, simple to use and scalable.* In addition, it can provide offline verification of paper-based transactions and goods without having to rely always on network connectivity.

2. MOTIVATING SCENARIOS

In this section, we describe three different rural supply chain scenarios which are in dire need of a low-cost security solution.

2.1 Drug tracking

Proper distribution of drugs is a huge problem facing developing regions due to weak laws for drug regulation and enforcement, erratic supply of medicines and unregulated markets. Theft of expensive drugs is rampant and counterfeiting of drugs is a commonly occurring extremely profitable business [3]. For example, one of the impediments in the implementation of highly active antiretroviral (ARV) therapy (HAART) for AIDS in African nations is the lack of accountability in the ARV drug supply chain. The World Health Organization (WHO) has argued the need for a drug tracking system that can monitor the flow of drugs from the supplier to the patient.

In Africa, many pharmaceutical companies provide expensive drugs at subsidized rates and the distribution of these drugs to patients through hospitals, health workers and health organization is fairly ad-hoc thereby leaving several loopholes in the system for theft and counterfeit drugs. To secure such a system, it is essential for the supplier to be able to track the flow of drugs at various levels in the supply chain till it reaches a patient. Such a system should be able to authenticate and uniquely identify drugs at every step in the supply chain. This type of remote tracking of the flow of drugs is currently lacking in developing regions.

2.2 Remote inventory management

In rural areas, agricultural supply depots are an important transaction center for a farmer. The farmer deposits his produce at the depot for long-term storage (to sell the produce during periods of peak prices when demand is high). In turn, the depots provide the farmer a receipt as a proof of the storage. Banks in developing regions have developed novel loan schemes where they provide the farmers with loans based on the storage receipts from depots.

However, these loan schemes have resulted in significant monetary losses in billions of dollars due to lack of repayments mainly due to fake receipts or the removal of produce in the depots (farmers store the produce, obtain the receipt and the loan but then remove the produce from the depot). The produce is manually registered in a notebook without any sort of authentication or identification mechanism both for the produce and the farmer. The accounts can be easily mismanaged or manipulated due to the lack of proper accounting procedures. Due to lack of proper inventory management procedures, the bank does not have any way of remotely tracking the farmer's produce in the depot.

2.3 Verifiable checks and documents

One of the challenges in rural microfinance service delivery is conducting financial transactions in remote rural areas [15]. Loans in the form of physical cash are distributed to people. Loanees typically have no safe way to store or transport cash, and often must travel quite far to collect it, as there are very few banks in rural areas. The loan officer has to personally meet every client and disburse the loan. This is not safe in rural areas [15]. For example, loanees typically pick up cash in pairs for mutual protection and officers must use private cars for safety (which is expensive). This results in delays and increase in expenditure to the bank or Micro-Finance Institution (MFI) and due to this cash transaction model, it leads to forgery and misappropriation of funds. At times loan officers also commit fraud [15].

A secure, low cost, paper based check that can be authenticated offline by loan officers (even if there is no network connectivity to the nearby city) and also authenticated by the bank would solve the problem of forgery and decrease the expenses of the bank or MFI.

3. DESIGN

In this section, we present our overall design of a secure supply chain system using paper, low cost microscopes and cell-phones.

3.1 Flow of the supply chain system

A basic rural supply chain system consists of goods or items that flow through various levels of hierarchies of suppliers, distributors and customers. We require a mechanism to track the goods at every level of the supply chain system.

The trusted central server or authority provides the goods, items or documents along with the paper tag for tracking and authentication. At every level in the supply chain system the goods along with their associated paper tags flow through the supply chain to the rural customer. At any point in the supply chain, the distributors, suppliers or central authority should be able to remotely track the goods,

thereby curtailing fraud and counterfeiting of goods. Also, at every point in the supply system, we require goods or items to be potentially verifiable in an offline manner without having continuous Internet connectivity. Our system does require intermittent connectivity to exchange "secure signatures" of goods across different supply chain points.

3.2 Architecture

The basic architecture of a secure supply chain management system is shown in Figure 1. The *central server or Trusted authority* distributes the goods, items or documents along with paper *Tags* which contains an identification component and an authentication component. The identification component may be a barcode or serial number and the authentication component is a speckle pattern which we will describe in detail in the next section. The *Tag* information of every item or supply is stored in the *central server*.

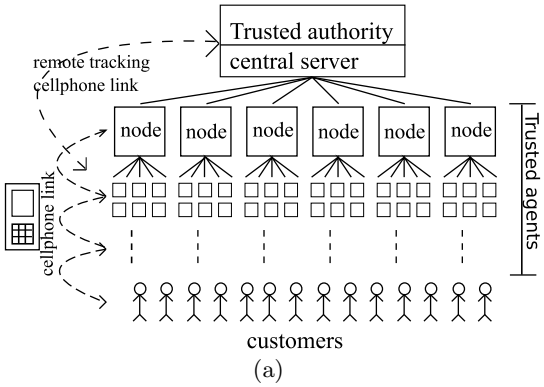
Each intermediary point in the supply chain is managed by an *Agent* who is equipped with a cellphone and a USB microscope that can be attached to the cellphone. Upon receipt of any goods, the *Tag* information is captured by the corresponding agent in the supply chain, who stores the *Tag* information in the cell phone. The cellphone acts as the local-store at each supply chain point.

The *central server or Trusted authority* uses cellphones to remotely track the flow of goods. This type of remote authentication is possible by transferring the *Tag* information attached to the goods, from a cell phone to or from the *central server* using SMS/MMS or GPRS connectivity. To verify the authenticity of a tag, an agent has three options: *online, offline, batch* authentication. In online authentication, the agent signals the tag information to the central server using the cellular network and verifies the authenticity of the tag. In offline authentication, the agent prefetches the list of "admissible" tags from the server into its local-store and verifies each tag with the set of admissible tags. In batch authentication, the agent can assume that the goods are genuine and merely store the tag information in the cell-phone locally. In this scenario, the agent can collect several tags and perform bulk verification in a lazy manner. An important benefit in this delayed batch verification is that it can significantly reduce the communication cost using cellphones and does not require immediate connectivity. In certain supply chain systems, such as the case of farmer receipts, online authentication is essential to sanction loans in real-time.

This architecture represents a distributed data-store of cellphones, where each node maintains a local store of authorized signatures and nodes communicate with each other using cellular connectivity. Note, that not all rural regions will have cellular connectivity. In such cases, it is essential for the agent to travel to a nearby location with cellular coverage to update the local-store and perform offline or batch authentication of goods.

3.3 Paper-based Authentication

An important aspect of our system architecture is *PaperSpeckle* [20], a low-cost solution we had previously developed to uniquely watermark any piece of paper. We use PaperSpeckle to perform paper authentication at every node in our supply chain system. *PaperSpeckle* requires only a simple low-cost microscope for authentication. While there have been several paper watemarking techniques based on the structure of paper in the literature [21, 4, 23], all these approaches are either extremely expensive or require special sophisticated machinery making them ill-suited for rural settings. *PaperSpeckle* is a paper watermarking mechanism that offers a tamper-resistant based authentication and identification of paper. *PaperSpeckle* improves upon two prior paper watermarking techqiues: (a) fiber fingeprinting by Metois *et al.* and Smith [21, 4], and (b) print signatures by Zhu *et al.* [23]. For a detailed description, refer to [20]. For completeness, we present a brief overview of the working of *PaperSpeckle*.



(a)

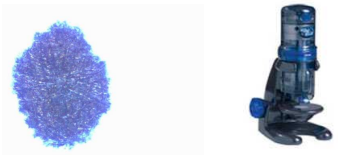
Figure 1: A generic design of paper tag based supply chain management system. The *Trusted authority* provides the watermarked paper *Tag* along with goods. Each node is managed by a *Trusted agent*. The *Trusted agent* uses the cell phone based *PaperSpeckle* mechanism to identify and authenticate items (goods, supplies or drugs or documents). *Trusted authority* can remotely track items at every node in the supply chain and check for fraud using the cell phone based system.

3.3.1 Working of *PaperSpeckle*

A speckle pattern is a random intensity pattern produced by the mutual interference of coherent wavefronts that are subject to phase differences or intensity fluctuations. These speckles are caused by rays scattering from different parts of the illuminated area. At the screen these rays have different optical path lengths; therefore the rays interfere and result in speckles. We use a consumer grade microscope: Digital Blue QX5^{TM}shown in Figure 2b, with inbuilt LED's and 10x-200x magnification to extract this speckle pattern from the paper.

It is difficult to observe and digitally capture speckles from a plain sheet of paper. So, a dark colored marker pen is used to strain a small region (of approximately 2mm) of the paper. This produces an arbitrary contour ink "blob" as shown in Figure 2a. The dark background (which is obtained from straining) helps to clearly distinguish bright and dark regions of the speckle, as compared to a light background. Due to arbitrary contour, there are two forms of "random" signatures: (a) a random speckle within the strained region; (b) an arbitrary shaped contour of strained region. This combination of two random patterns is hard to forge.

After digitally capturing the speckles using the microscope, SIFT [12, 11] image matching algorithm is used to extract feature information of all the speckle images stored in the repository. For matching two speckle images, say a and b, we use SIFT and match feature information of a with feature information of b. If the match is greater than a cer-



(a) (b)

Figure 2: (a) An arbitrary shaped speckle. Straining a small region of paper with colored marker pen and using Digital Blue QX5^{TM}(b) to digitally capture the speckle at 60X magnification.

tain threshold [20], then speckle a is equal to speckle b.

The properties of *PaperSpeckle* that makes it suitable for authentication purposes in developing region environments are: i) Low cost: At each point or node in the supply chain, the equipment used to authenticate goods are a paper *Tag* which is attached to the supply and a low cost microscope (retail price around $99). ii) Portable: Paper and microscope are both portable, so this ideally fits the ad-hoc nature of supply chain systems in developing regions. iii) Tamper-resistant: In developing regions, paper might be poorly maintained due to bad storage environments, damage due to rain, crumpling of watermaked area and aging of paper. But, we have stress tested *PaperSpeckle* and shown that it is quite robust in the wake of extreme conditions: (a) many crumplings around the watermarking region; (b) soaking the paper in water; (c) extracting the signature under different lighting conditions; (d) aging of paper across time.

3.4 Low-bandwidth challenge

Building a distributed system using cellphones alone raises several interesting research challenges. First, cellular networks support very low operational data rates, often lower than the data rates offered by dial-up connectivity. Second, cellphone connectivity is intermittent due to two reasons: (a) not all regions have cellphone connecitivity requiring the agent to travel; (b) even with continuous cellular coverage, high bandwidth prices forbid a user from using it continuously. Given the low-bandwidth, intermittency and high usage cost constraints, we have to be very careful about the utility of every bit transmitted on the wire.

One challenge we are working towards is to address the problem of how to efficiently verify in very low bandwidth environments. Especially, in the cellphone case, we are restricted to GPRS, SMS or MMS links for data transfer. After different lossy compressions and image extractions, we can reduce the size of a speckle image to about 5 KB. If we use GPRS connectivity, we can verify the authenticity of a speckle in the order of a few round-trip times. However, if we restrict ourselves to SMS connectivity, we are constrained with about 160 bytes. We are working on mechanisms that would enable us to encode a paper tag along with the speckle information within one SMS message. Otherwise, we can definitely split the image across different SMS messages. If bulk deals for SMS are available, we can use SMS as a cheaper means of transport than GPRS connectivity. Alternatively, if MMS service is available, as is the case in certain regions, we can transfer the speckle image in one shot. Also, we can perform offline and batch authentication using GPRS or MMS service at much lower costs. One problem with MMS is the high usage costs. Kiva [10] has been experimenting microlending with MMS and tagging service [7] and this approach has been effective with the local partners but the usage costs of their system have been fairly high.

3.5 Current Implementation

We have developed *PaperSpeckle* and have rigorously tested its properties across various types of paper and various tampering mechanisms. We have ported PaperSpeckle to work on top of Google's Android [5], an open platform for mobile devices. The overall system is functional and we have implemented basic compression routines to reduce the size of speckle images. More work needs to be done in minimizing the overall cost for bandwidth consumption. We are working with the West Africa AIDS Foundation in Ghana and a well established microfinance institution in India and hope to deploy a version of our system soon.

3.6 Comparison to alternatives

The two forms of paper based authentication and identification systems that are commonly used are, 1) Barcodes and semacodes; 2) Paper checks or bank checks.

Barcodes and semacodes are commonly used in supply chain systems to track the flow of items and goods. As each barcode is unique, it can identify a specific item. But, barcodes can be easily copied or cloned, due to which it lacks secure authentication property.

A paper check (bank check) can have two important security properties, 1) hidden watermarks, and 2) random numbers that uniquely identify each check. The watermarks are embedded within the paper check and these watermarks are later read as a part of authentication process using special purpose machinery. The random number uniquely identifying each paper check or any sort of unique number identifying a paper check exposes the system to simple copy attacks.

PaperSpeckle, uses the intrisic property of the paper to uniquely identify and authenticate each paper, thereby providing better security and preventing any copy attacks. Also, the paper can be authenticated using a cellphone and a simple microscope, without the need of any additional machinery.

4. SOLUTIONS

We now briefly describe how our cell-phone based paper authentication system that aid in improving the security of the three supply chain problems discussed in Section 2.

4.1 Drug tracking

To address the drug tracking problem, we use paper *Tags* which contain two fields; 1) a barcode that identifies the bottle of drug based on its name, quantity, batch number and so on and 2) a speckle pattern for authentication. This combinational tag helps in uniquely identifying every bottle along with its contents. The
$\langle barcode, speckle \rangle$ *Tag* is provided by a *Trusted authority* (the company manufacturing or marketing the drug). A counterfeiter may generate a legitimate barcode but cannot spoof the speckle pattern corresponding to the barcode. The speckle aids in attaching a physical authentication to every bottle which was not present before. If the tag is well attached to the drug, physically removing a genuine tag and attaching it to a counterfeit drug should be fairly cumber-

some. In addition, if paper is stuck to some material, the process of detaching the paper from the material does affect the fiber structure which in turn may affect the speckle pattern considerably. We have not experimented in detail with these forms of tampering with PaperSpeckle to equivocally state that we can detect label removals. One type of theft we cannot deal with is that the medicine could be physically removed from the bottle or strip and replaced with a counterfeit medicine. One needs clever packing methodologies to ensure that once a case is opened, it can be easily detected.

4.2 Remote inventory management

To solve the remote inventory management problem, we use the following paper *Tag*: $\langle number, speckle \rangle$. The *number* can be a serial number and *speckle* is the unique speckle pattern for that supply. Using this tagging mechanism it is easy to identify, authenticate and maintain records in a warehouse. The paper *Tag* is provided by a *Trusted authority* such as the rural bank or the rural agricultural society. And the *Local merchant* scans the *Tags* once they are attached to the supply (like a bag of rice). Due to this $\langle number, speckle \rangle$ *Tag* approach, every bag of rice or supply in the warehouse can be tracked and authenticated by the rural bank when its *Trusted agent* comes in for inspection or remotely using cell phones.

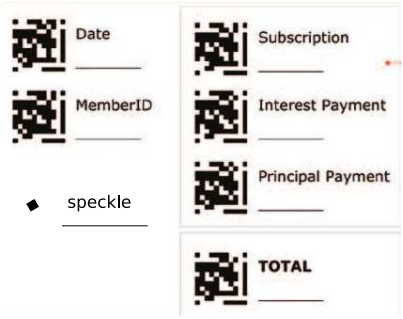
This approach has certain limitations: i) paper *Tag* may be removed from the supply or item, ii) malicious agent might scan the *Tag* for remote authentication even though, there may not be any supply at all. To address the latter problem, one can envision sending a trusted agent to the depot to perform "random" checks on specific tags; if the trusted agent finds a malfunctioning depot, that depot can be disabled for future transactions.

4.3 Offline checks and documents

Paper based checks can be provided by a *Trusted authority* such as bank or an MFI to the loanees which can be authenticated and checked by a *Trusted agent*. The paper check contains the loanee's name, amount, date encapsulated in a barcode and a speckle pattern that prevents the loanee from cloning the check. CAM [14] forms can be used for identification purposes. The *Local merchant* checks the loanee's name, amount and date using a CAM enabled cell phone and then authenticates the CAM form by examining the speckle pattern on the form. The *Local merchant* checks the loanee's speckle image with all the original images in his cell phone repository. If the speckle matches, then the form is original and is not a clone. By checking the CAM visual codes and speckle pattern, the *Local merchant* is certain of the identity of the loanee and authenticity of the check. A CAM form with speckle patterns is shown in Figure 3. A similar approach can be used to check identity and authenticity of paper based medical records. The person's name, age, birth date can be encapsulated in a barcode to check the identity and a speckle pattern to check for authenticity of the document.

5. RELATED WORK

There have been several industrial efforts that have used barcodes and RFIDs to perform efficient and secure supply chain automation systems for inventory management [13, 22]. Many of these solutions require sophisticated machinery which are well beyond the reach of rural developing regions.



(a)

Figure 3: CAM based check with speckle pattern for offline authentication. The CAM form is provided by the *Trusted authority* (bank or MFI). The loanee cannot duplicate or copy the form because of uniqueness of the speckle pattern. Identification of the loanee is done using a CAM enabled cell phone which contains the loanee's id (MemberID). And authentication is done by comparing the speckle image with already stored original speckle image in cell phone repository of the *Local merchant*

Hence, a detailed description of these systems is outside the scope of this paper. Our work in contrast to these systems has adopted a practical approach using very low-cost devices to build a tractable paper and cellphone based secure supply chain system.

Several works have experimented with cell-phones in rural regions. Parikh et al [14, 16] introduce CAM, a successful mobile user interface toolkit which is used in rural microfinance across India. The 2-D visual code that can be scanned by a camera phone was introduced by Rohs et. al [18] and is presently being used in CAM. Cooltown project [9] uses RFID, barcodes and sensor devices to retreieve specific HTML documents.

Apart from PaperSpeckle, there are other types of physical authentication systems. Pappu [17] introduces physical one way functions using lasers and its application to tamper-resistant physical authentication systems. Zhu et al [23] describe a way of authenticating printed paper using profile matching techniques. The printing process produces some non-repeatable random profiles for each paper that is printed. Metois *et. al.*[4] propose FiberFingerprinting which uses fiber structures present in the paper to produce unique hash strings.

6. CONCLUSIONS

Today, rural supply chain systems operate in an ad-hoc manner with poor accounting practices and hence are susceptible to security threats. These systems are in need of a low-cost security solution that can aid in curbing the level of theft and fraud. In this paper, we have proposed one such security approach which relies on very low-cost and easy to use machinery: cell phones, microscope and paper. We believe our system is easy to deploy. While we have developed an initial version of our system, still much work needs to be done to make it practical and usable in real-world settings. We work closely with institutions in India and Ghana and are hoping to deploy our system in these places.

7. REFERENCES

[1] FDA 2004 Feb. http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html.

[2] ITU News Magazine. Jan-Feb 2008. Mobile phones for half the worldâĂŹs population. http://www.itu.int/itunews/manager/index.asp?lang=en.

[3] AllAfrica 2008 Feb. http://allafrica.com/stories/200802070170.html.

[4] N. Salzman E. Metois, P. Yarin and J. R. Smith. Fiberfingerprint identification. In *Third Workshop on Automatic Identification*, 2002.

[5] Android Platform from Google™. http://code.google.com/android/.

[6] Remote Transaction System in Uganda:. http://www.microfinancegateway.org/content/article/detail/19145.

[7] Ravi Jain. The mobile web in developing countries. In *W3C Workshop on the Mobile Web in Developing Countries*, 2006.

[8] Matthew Kam and Tu Tran. Lessons from deploying the remote transaction system with three microfinance institutions in uganda. In *Proceedings of UNIDO-UC Berkeley "Bridging the Divide" Conference*, 2005.

[9] Tim Kindberg. Implementing physical hyperlinks using ubiquitous identifier resolution. In *WWW '02: Proceedings of the 11th international conference on World Wide Web*, pages 191–199, New York, NY, USA, 2002. ACM.

[10] Kiva. http://www.kiva.org.

[11] D. Lowe. Distinctive image features from scale-invariant keypoints. In *International Journal of Computer Vision*, volume 20, pages 91–110, 2003.

[12] David G. Lowe. Object recognition from local scale-invariant features. In *Proc. of the International Conference on Computer Vision ICCV, Corfu*, pages 1150–1157, 1999.

[13] OATSystems. http://www.oatsystems.com.

[14] Tapan S. Parikh. Using mobile phones for secure, distributed document processing in the developing world. *IEEE Pervasive Computing*, 4(2):74–81, 2005.

[15] Tapan S. Parikh. Rural microfinance service delivery: Gaps, inefficiencies and emerging solutions. In *International Conference on Information and Communication Technologies and Development, 2006. ICTD '06*, pages 223–232. IEEE, 2006.

[16] Tapan S. Parikh, Paul Javid, K. Sasikumar, Kaushik Ghosh, and Kentaro Toyama. Mobile phones and paper documents: evaluating a new approach for capturing microfinance data in rural india. In *CHI*, pages 551–560, 2006.

[17] Pappu Srinivasa Ravikanth. *Physical one-way functions*. PhD thesis, Massachusetts Institute of Technology, 2001. Chair-Stephen A. Benton.

[18] M. Rohs and B. Gfeller. Using camera-equipped mobile phones for interacting with realworld objects, 2004.

[19] CGAP IT Innovation series:. http://www.cgap.org/docs/it_pda.html.

[20] Ashlesh Sharma, Lakshminarayanan Subramanian, and Eric A. Brewer. Paperspeckle: A low cost tamper-resistant paper watermarking. Technical Report TR2008-909, Courant Institute of Mathematical Sciences, New York University, December 2007.

[21] Joshua R. Smith and Andrew V. Sutherland. Microstructure based indicia. In *Proceedings of the Second Workshop on Automatic Identification Advanced Technologies*, pages 79–83, New York, NY, USA, 1999. ACM.

[22] Unisys. http://www.unisys.com.

[23] Baoshi Zhu, Jiankang Wu, and Mohan S. Kankanhalli. Print signatures for document authentication. In *CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*, pages 145–154, New York, NY, USA, 2003. ACM.