RESEARCH ARTICLE OPEN ACCESS

A Review: Strategies for Recognizing Forgery in Identity Documents

Alsadig Bashir Hassan Abass, Yahia A. Fadlalla
College of Computer Science and Technology Sudan University of Science and Technology
SUST Khartoum - Sudan
Lead Consultant/Researcher InfoSec Consulting, Hamilton, Ontario - Canada

ABSTRACT
Discovery of fraudulent documents as of late has ended up crucial as techniques to form these fake documents are getting to be broadly open and basic to utilize; indeed, for an untrained person. A promptly and effortlessly available gigantic writing that contains basic data on recognizable proof cards, birth certificates, or identifications has continuously exacerbated the issue. This promptly accessible writing portrays various strategies and procedures that favorably bolster the making of fake IDs and documents. This overview paper investigates various strategies for countering archive fraud dangers in conjunction with their accomplishments and restrictions. At the final of the paper, there's a table that compares these strategies. Novel and more successful procedures and strategies are required to resolve and control the threats and dangers of IDs and reports imitation.
Keywords*:* - IDs, character card, extortion, imitation, international id, detection, fake, watermarking, biometrics, records, printer sort.

I. INTRODUCTION

Presentation the Identity Document (ID) is utilized to recognize a person or affirm him or her points of view, for example: title, sex, nation, age, ID number, etc. The number of countries issue formal identity records though others require identity confirmation utilizing casual archives. Those IDs such as National Recognizable proof Cards, Driving Licenses, Home Cards, Travel permits, Marriage Certificate, Alter of Title Certificate, Military Recognizable proof, Birth Certificates, Passing Certificates and the like [1][2],[3]. Falsified ID is based on the establishment of imaginary data, frequently can be by combining veritable data with created information. For occasion, the counterfeiter may take one's individual title, combine it with another person's address, and utilize somebody else's nation to make current personality record. The guilty party can at that point utilize this manufactured character to apply for credit, make major buys, or a distinctive other exercise that terrific the personality a budgetary history [4].

Due to the advanced change of progressed quality computers, printers and scanners, which are comparatively of cheap taken a toll, ID's extortion got to be a mind-blowing issue these days. Fakes IDs overwhelm over the globe, a few cases are human traffickers, dread assaults, sedate bootleggers, and unlawful migration. Agreeing to [5], in 2019 there are around 16.7 million casualties of character extortion and $2,100,000,000 in gauges misfortunes. Many analysts have examined these chance and displayed unmistakable methodologies for ceasing, keeping up or handling it. Hence, in this survey paper, we looked into the past and afterwards strategies that are utilized to discover ID imitation. The rest of this paper is organized as takes after: Area II gives a brief around a few security strategies for ID cards and we show an exhaustive examination of the current strategies for countering report imitation dangers and examines their accomplishments and restrictions in Area III. Area IV the conclusion of the paper, and area V a table that sheds lights on a few strategies and strategies that checked on and provide comparison them.

II. SOME TECHNIQUES TO SECURE THE ID-CARD

Working in a high-security environment considers taking measures to secure your organization's ID card printer and program against robbery or unauthorized utilize.

(1) Printer Types: A few printers can make a few security highlights on the cards, such as serial numbers, date of printing and the shape of the characters or designs.

(2) Software Instruments: It is a critical thought for anticipating illegal duplication and altering of the ID card by utilizing a few programs as security include that ranges from watermarks; which are nearly translucent in their appearance and are connected by hand or by forte watermark-capable printers, depending on how the ID card is held and where the light hits it, you'll be able to see the watermark in certain points. To 3d image Stickers; which are self-adhesive patches that are connected to the card after it is printed. You'll be able to select from a combination of full plans, which include to the solidness of your ID

identifications as well. To cover; which is considers as another.

III. RELATED WORKS

This segment briefly surveys later and past related work on methods of recognizing imitation in character archives.

A modern displaying approach for confronting morphing assaults for photo- ID reports is presented in [6]. On the premise of these displaying approaches, two distinctive realizations of the confronting morphing assault, as well as a scientific morphing locator, are executed and assessed. The plan of the included space for the finder is based on the thought that the mixing operation within the morphing pipeline causes the reduction of confronting points of interest. The most commitment of the approach could be a novel and pertinent strategy for demonstrating the application setting of photo-ID reports assaults and planning the fitting media legal finders. Moreover, it permits for characterizing the prerequisites for report checking. The show of the morphing assault appears that the risk can be decreased by avoiding a client from submitting pictures into Report Era forms.

This model utilized to compare diverse confront morphing assault realizations and to determine the designing prerequisite for morphing locators. Be that as it may, A encourage illustration of a vital operation that would have to be secured in future inquire about is print and check operations.

Authors in [4] looked into a number of papers almost a few strategies that commonly utilized for recognizing imitation on identity documents. These strategies such as Computerized Watermarking; which could be a handle insert information into a mixed media question to secure the one's possession to the protest. The other category is based on human recognition can be unmistakable or imperceptible watermarking. A third category based on the strength that's how the watermarking stands up to the assaults. In expansion, they talked about the Biometrics; whish is interesting physical or behavioral characteristics that utilized to confirm individual character. Biometrics separates into Physical characteristics and Behavioral ones. Besides, they examined Steganography: It could be a science of covering up data by implanting messages interior the content, picture, sound, or video. The creators demonstrated that the discussed methods and strategies have disadvantages, so more work in this field is exceedingly energized to relieve the chance behind these dangers, more ID discoveries strategies must be looked for and made accessibly. In any case, the work of cryptography (e.g., watermarking) must be empowered in recognizing ID fraud or making existing ID-making methods more secure.

In [7], the authors make a arrangement for recognizing forged text-documents that's called Copy-Move Fraud Location (CMFD). The copy-move is to duplicate a portion of text-document and reinsert it one more in another range within the same text-document. This point to cover undesirable contents or replicated extraordinary portion, e.g., to make unused names, dates or values. CMDF comprises of two parts: (1) Optical Character Acknowledgment (OCR), centers on recognizing text style fraud by measuring their weight, measure, fashion and unpleasantness. (2) Duplicate Move (CM), which is centering on the foundation of the content record. Be that as it may, CMDF would be more exact on the off chance that utilizes a Conditional Irregular procedure.

A programmed imitation location strategy based on record text style highlights is displayed in [8]. The strategy is based on a Conditional Irregular Field show which, to begin with, permits us to recognize and classify typefaces and after that to highlight text style imitations. The framework can recognize three sorts of mistakes, to begin with, Copy/paste: the space between a match of characters varies from the ones between the rests of the combination of characters, it can be littler or greater; Moment, Impersonation: a single word shows up to be composed in two distinctive typefaces; Third, Copy/paste and Imitation: both mistakes, above described, can be found within the same word. Be that as it may, as the creators proposed, including data relative to the neighboring words may increment the textual style acknowledgement rate and maximized textual style imitation location.

A ponder to form ID card for European Union (EU) citizens more grounded by utilizing EKSISTENZ extend is proposed in [9]. They consider displayed the introductory extend created almost the conceivable powerless focuses which exist along the ID lifecycle the venture will center on the citizen, to propose arrangements to avoid, identify, react and recoup from a personality imitation and robbery episodes. A few instruments of EKSISTENZ venture centered on to begin with issuance, utilization, reestablishment and denial forms. These tools are based on Biometrics, because it will give a secure and univocal way to relate the ID card with the client, both within the issuance and within the regular utilize. A few other devices for securing the client, the information stored, using both biometrics and cryptography. Other apparatuses of EKSISTENZ venture for cases of repudiation, reestablishment, and to form less demanding the announcing of conceivable ID imitation and robbery and the other one to secure the connection between auxiliary and essential IDs in case of the former's burglary.

A framework to find the fake photocopied record by utilizing Bounding Box (BB) is displayed in [10]. This framework center on the portion of archive that has been altered by evacuating the first substance and composing over it or changing the substance by cut and glue procedure. BB employments Matlab apparatus to encompass the characters and images locales to distinguish fraud on the archives by the stature, introduction, and thickness on the record, if there's a distinction within the suspected portion of the archive; at that point the framework recognizes a fraud. In any case, as this framework may take well much time amid the comparison handle.

A scheme to distinguish the forged reports by centering on the foundation region and photo area is proposed in [11]. This plot recognizes an uncommon kind of ink that was utilized amid the printing prepare. On the other hand, the system identifies imitation on the printed photo by recognizing the printer utilized to print that photo. Inkjet printers illustrate manufactured archives and laser printers illustrate unique archives.

A system to distinguish the source of the printers is proposed in [12] it depends on the clamor made by the printer, in any case of the substance and the estimate of the

report. The proposed framework separates the inkjet printer to shape other printers.

A proposition for an academic card based on ICAO standard contributing to the concept of league is proposed in [13]. The ICAO 9303 standard could be an arrangement of records made by the Universal Gracious Flying Organization (ICAO), which points to portray the determinations for a Machine Clear Travel Reports (MRTDs). The MRTDs that take after the 9303 standards utilize a machine-readable zone (MRZ) to encourage the assessment of reports. Within the MRZ is contained key data almost the record, the issuing state, and archive number. Moreover, it contains the client information, such as date of birth, sex, nationality, other than the expiry date of the report conjointly, the title of the archive holder. The scholastic league includes instructive and inquire about educate. It permits individuals connected to these teaching to share data and assets and get to confine administrations. In any case, the Machine-Readable Travel Document (MRTD) standard employments contactless Coordinates Circuit (IC) is defenseless to a few assaults. For illustration, the information can be electronically perused without authorization inside a remove of a few meters.

A keen apportion card utilizing Radio Frequency Distinguishing proof (RFID) method and Worldwide Framework for Portable Communication (GSM) method to anticipate the apportion imitation is created in [14]. Apportion card may be an exceptionally essential archive for each citizen in India. Apportion card is utilized to buy different essential things like sugar, oil and the like, from the proportion shops at a cheaper rate, issued by the government. Proportion card acts as the address/identity confirmation of an individual. It includes the personality of the individual besides his family individuals, their names, ages, sexual orientation. Agreeing to the number of individuals within the family, the proportion will be given in that proportionate proportion. But, the current ration card framework includes a disadvantage, that on the off chance that the things are not sold up to the final of the month, at that point the businessperson will offer it to somebody else and take the benefit into his take and put a few wrong perusing within the government record journal. The proposed framework evacuates the fraud by evacuating the manual filling of the government record journal with the RFID and GSM framework. The GSM framework sends data around the conveyed apportion to the government office conjointly by the enrolled number of the client and the record will be kept up by the online framework. In any case, this framework is confronting certain confinements like fetched is tall.

Fig. 1: Image represents the current ration card [14]

The analysts in [15] utilize a system to distinguish produced photocopied archives by Geometric Minutes and Gray Level Co-occurrence Framework Highlights. They concentrate on identifying manufacture that happens within the report in which some substance of the first substance has been modified or overwritten. The strategy can identify the extortion in a document by its steady concentrated; on the off chance that it is smooth and has solid edge form, it illustrates a non-fabricated photocopied content; in case it is harsh or includes a powerless edge form, it illustrates a manufactured photocopied content. The framework in [30] is additionally utilized to improve the reports by making it free of clamor and soil.

A strategy permits programmed comparison and interpreting of Fake Assurance Framework (CPS) codes are presented in [16]. The CPS or machine recognizable proof code (MIC); is interesting for each printer and can hence be utilized to recognize the gadget that was utilized to produce the print-out. This work considers an expansion of the past work on CPS code classification. The CPS codes comprise of little yellow dabs that are imperceptible to the unaided human eye. These specks frame a design that's rehashed numerous times on a page with a settled even and vertical dispersing.

These designs contain information around the printer that was utilized to create the print-out, e.g. the serial number of the gadget. In the event that designs are indistinguishable, the addressed archive comes from the same gadget. In the event that they vary, it can be concluded that the record comes from a distinctive source. By that as it may, in spite of this work, the assessment would advantage in the event that too the interpreting of the designs other than the Xerox sort would be known.

A ponder of documents counterfeit methods by analyzing the security components is displayed in [17]. They centre on the falsifying of travel archives by distinguishing the security components. In this reason, there are displayed both the Security components and print strategies utilized in travel archives and strategies of adulteration and measurable inquire about of these archives. Approximately the Security components and print strategies utilized in travel reports, utilize check just like the watermark. Other security highlights are the idle picture, the retro-reflective picture, the optically variable picture, the covered-up picture, fluorescent impressions, kilograms, visualizations, the thread-safe, strands, planchettes, the encoded picture, too, the encoded picture that incorporates person data approximately the holder's title, report number, date of birth, which are coordinates into the photo or inactive data such as the title of the nation, coordinates into the foundation of the drawing.

Fig. 2: Image (a) is an authentic document [17]

Fig. 3: Image (b) is a fabricated document viewed in a white light [17]

An approach for programmed record imitation discovery by recognizing twists that are commonplace for filtered or re-engineered reports is presented in [18]. The location of the twists is done on fixed-document parts, e.g. headers and footers that frequently show up in solicitations. Given a set of archives from the same source, without earlier data almost which report is honest to goodness and which isn't, they are all coordinated against each other. The whole of the coordinating scores is utilized as a highlight to identify exceptions in a cluster of reports from the same source. The thought behind this approach is the taking after: solicitations regularly have common text parts that don't shift over distinctive solicitations, as e.g. headers and footers. Filtering twists and loose re-engineering will change somewhat the relative position of these content parts. By coordinating all records in a cluster against each other, the whole of the coordinating qualities for each archive can be computed. The fashioned record will have a lower score due to the checking mutilations.

A strategy for consequently extricating and classifying the counterfeit assurance framework (CPS) codes for color laser printer and copiers is displayed in [19]. To anticipate the utilize of color laser printers or color copiers for falsifying e.g. cash, ID cards or other profitable reports, numerous of these machines print Fake Security Framework (CPS) codes on the page. These little yellow specks encode data almost the particular printer (e.g. sort of printer, the serial number of the gadget.) and permit the addressed report inspector in participation with the producers to track down the printer that was utilized to create the archive. Moreover, it contains data around the printer that was utilized to produce the print-out, e.g. the serial number of the gadget.

A strategy characterizes both intrinsic and extrinsic highlights as a composite signature utilizing the Benford's law based on, to begin with, digit insights to multi-size square DCT coefficients for printer recognizable proof portrays in [20]. Geometric mutilation marks speak to the composite highlight brought about both by halftoning and electrophotographic (EP) printer mutilation. Such geometric twisting marks do display a tall relationship with comparing printer marks and a moo relationship with other printer marks. They propose to apply Benford's law based on, to begin with digit insights to multi-size piece DCT coefficients for printer distinguishing proof, which utilize to diminish the arbitrary commotion effect, a white edge is expelled at each filtered picture since the checked picture estimate is bigger than that of the test picture. By averaging Benford's law insights on the number of duplicates of the test picture to diminish arbitrariness. The commitments of their work are: (1) Create multi-size block-based DCT coefficients Benford's Law for legal highlights extricated from printed reports. These highlights are utilized for printer distinguishing proof. 2) Composite signature considers both the impacts of halftoning and printing mutilation. 3) Utilize of bolster vector machine (SVM) classifier to distinguish the brand and show of printers. In any case, as the creators said by creating blended legal highlights for printer demonstrate recognizable pieces of proof in conjunction with clamor highlights in printed records it'll more secure.

A framework which considers a novel recurrence space approach for record printing procedure acknowledgement that makes a special unique finger impression for each printing innovation from the number and dissemination of the frequencies contained in an archive created in [21]. The test comes about to illustrate that utilizing discrete cosine change (DCT) coefficients and machine learning methods can offer assistance recognize between inkjet-printed and laser-printed reports conjointly distinguish first-generation photocopies at moo filter resolutions. They found out that the laser-printed report picture is characterized by sharp moves between character and non-character regions. In differentiate the photocopied and the inkjet-printed pictures appear an inclination towards smoother and obscured character edges. This highlight is due to printing substrate dissemination within the case of the inkjet-printed picture and light diffusion amid checking within the case of the photocopied archive since the photocopy prepare has at slightest two particular stages: filtering the format report and printing the filtered substance. On the other hand, a tall degree of edge harshness is watched for the inkjet-printed record; in differentiate, small edge harshness is seen for the laser-printed record.

In [22], a framework to identify fraud on checked archives based on covering up procedures is proposed. Steganography is one of the data covering up procedures; it is the science of imperceptible implanting of data in a computerized medium. In any case, Steganography's frameworks require a parcel of overhead to stow away generally few bits of information.

One of the common procedures in recognizing the visa imitation is based on the Machine Lucid Zone (MRZ) is portrayed in [23]. MRZ is exceptionally basic in visa

acknowledgement, which is set on the foot of the international id. On the off chance that the data within the visa matched with MRZ code isn't indistinguishable, meaning the international id is falsified.

An approach for identifying misrepresented records employing an archive signature gotten from its natural highlights: bounding boxes of associated components are utilized as a signature is displayed in [24]. Utilizing the demonstrate signature learned from a set of unique bills, the approach can distinguish reports whose signature essentially contrasts from the demonstrate signature. The approach works as takes after: observing a number of unique bills from one receipt party permits building show signs of the non-variable portion (e.g. headers, footers, source address and phone number) of a charge. A modern charge is at that point checked against this show signature and in case it is altogether diverse, it is considered as a possibly faked charge. The approach employments all-inclusive ideal record arrangement to construct a show signature that can be utilized to compute the likelihood of a unused archive being an unique one. Be that as it may, the strategy has the advantage that no additional security highlights ought to be included either to the paper or to the printing prepare.

A show for lessening the discovery mistake rate of printed images, in cases where the luminances of the images depend on a message to be transmitted through the Print and Check (PS) channel, is displayed in [25]. This work proposes a confirmation convention for printed and computerized archives, where it is conceivable to decide whether one or more characters have been adjusted in a content record. The skewness measures the degree of asymmetry of conveyance around its cruel, it is zero when the dispersion is symmetric, positive on the off chance that the dispersion shape is more spread to the proper and negative in case it is more spread to the left; while the kurtosis may be a degree of the relative levelness or peakedness of dissemination approximately its mean, with regard to an ordinary dispersion; tall kurtosis dissemination contains a more honed crest and compliment tails, whereas a moo kurtosis dispersion features a more adjusted top with more extensive “shoulders,”. In any case, take note that the commitments displayed can be combined with other strategies, serving as a viable elective for record authentication.

A framework portrays the utilize of picture surface investigation to recognize the printer utilized to print a record, in specific, portrays a set of highlights that can be utilized to supply measurable data approximately an archive is displayed in [26]. They treat the yield checked record as an “image” and utilize picture investigation apparatuses which are the grey level co-occurrence surface highlights to decide the highlights that characterize the printer. This device can extricate the features of “e”s within the report. The reason for this can be that “e” is foremost as often as a possible happening character within the English dialect. A set of highlights are extracted from each character-shaping a highlight vector for each letter “e” within the archive. Each highlight vector is at that point classified separately employing a 5-Nearest-Neighbor (5NN) classifier. The 5NN classifier is prepared with a number of include vectors. Be that as it may, it is vital to note that the method displayed requires that earlier data around the printers in address be known. In case the obscure document was printed by a printer which isn't included within the classifier preparing information set, at that point, it will be erroneously be classified as one of the known printers. It will too be important to amplify this strategy to work with different text style sizes, textual style sorts, conjointly distinctive characters.

A scheme relates to a handle for warm exchange printing a recognizable proof card to deliver a metallic thwart security highlight on the card is displayed in [27]. The strategy comprises the steps of a) giving a card substrate having a warm exchange dye-receptive surface; b) giving a set warm color exchange boards counting a metallic thwart board; c) printing indicia onto the dye-receptive surface; and d) printing a metallic border along the outside edges of chosen printed indicia to form a metallic security format around the chosen indicia. The chosen printing include is basic since it requires a significantly correct and exorbitant print motor to accurately align the pixels to achieve the required effect, though lesser exact warm printing contraptions will tend to take off messy edges which promptly detectible to somebody recognizable with the security include.

A scheme for providing strategies and device to uniquely determine fabrication details related with objects, such as recognizable documents, work of art and restricted issue works, utilizing open cryptographic procedures is displayed in [28]. A cryptographic signature is made by a private key. The private key is extraordinarily related with creation points of interest such as a workstation, administrator, manufacture hardware, manufacture materials and the like. An open key compare with the private key; and thus, the open key is related to the manufacture of subtle elements. The confirmation operation makes by translating the cryptographic signature with the open key extraordinarily in arrange to recognize the manufacture of subtle elements. In any case, this plot bargains as it were with an immaculate content record. It may fall flat to identify picture imitation.

A scheme that gives frameworks and strategies for including delicate and strong watermarks to a unique report because it is printed that can be by printing a document requiring fraud assurance employing a number of trusted printers is displayed in [29]. A larger part of printers is overseen by a print administration framework. Each printer can give numerous security advances. The approach decides the assurance advances for the archive to be printed. The print administration framework courses the print work to a printer that can apply the reasonable assurances and sets the appropriate parameters inside the printer. Duplicate prove that can set up that a report may be a fraud and/or following data that distinguishes the overseer of the archive and restrictions on replicating of the document and utilizes of the information within the record are included within the watermark that's printed on the report. A record can be verified as a unique or set up as a fraud by checking on the duplicate prove and/or following data within the watermark. In any case, advanced watermark has a few shortcomings; expulsion assault that point to expel all watermarking; cryptography assault that point to change watermarking, and convention assault that point to assault all watermarking applications.

A framework to secure print and follow reports on moo fetched shopper printers such as inkjet and electrophotographic (laser) printers are presented in [30]. They created two procedures for printer recognizable proof based on analyzing a printed archive. The primary procedure is inactive; it includes characterizing the printer by finding natural highlights within the printed archive that are characteristic of that specific printer, demonstrate, or manufacturer's items, which allude to it as the natural signature, that requires an understanding and displaying of the printer instrument, and the advancement of investigation instruments for the location of the signature in a printed page with self-assertive substance. The moment methodology is dynamic, that can be by inserting an outward signature in a printed page that produces by balancing the method parameters within the printer instrument to encode distinguishing data such as the printer serial number and date of printing.

An unused strategy based on making computerized pictures with particular properties, called a Duplicate discovery designs (CDP) which is dependable and cost-effective arrangement that's printed on self-assertive records, bundles and others is proposed in [31]. It is generally embedded within the computerized picture of the record to be printed, or straightforwardly printed on the archive; CDPs are not suited for naked-eye discovery. Each time a picture is printed or scanned; a few data is misplaced almost the first advanced picture. By measuring the sum of data contained in a checked CDP, the CDP finder can take a choice on the realness of the report, without a CDP those reports would be simple to duplicate and fake. In any case, the utilize of laser etching and 3d images, for illustration, are other appropriate carriers for the CDP will be more secure.

A multilevel security-device based on BR as a fabric for open highlights as well as machine-readable highlights among them information capacity is displayed in [32]. There are distinctive highlights combined in BR. To begin with, it appears a recognized photochromic impact which is giving an effortlessly perceptible color alter within the unmistakable wavelength administration. In expansion, the fabric may be utilized as a polarization-sensitive capacity fabric. The capacity effortlessly realistic on e.g. ID-card is within the run of a few megabytes of information. Moreover, an optical information encryption strategy has been created which permits productive information assurance from unauthorized reading; that can be by overwriting of the primary data with moment data can be utilized for optical information encryption. An ID-card carries obvious and undetectable security highlights based on BR is tried. Beneath the distinguishing proof information and the picture, the full card is coated with a lean layer of BR which nearly is imperceptible by the exposed eye but is effectively machine-readable. This include is utilized to test the realness of the substrate. A field on the ID-card made from BR but here a strongly color is connected by screen-printing or cushion printing. This field is utilized for communication with the client. In verification terminals, data can be recorded on this message field. After a couple of minutes, it vanishes. Indeed, within the case of a misfortune of the ID-card, the data does not get accessible to any other one. This field can too be utilized for authentication purposes because it changes color upon light with light. This will be checked with daylight or indeed a burn. Another field on the ID-card features a moo capacity information capacity field. The data is put away as diverse polarizations and for this reason, may not be recognized by the bare eye. In this field, the picture of the card proprietor for illustration and his information in computerized frame are put away. There's sufficient capacity to store in expansion to unique mark information or therapeutic information or anything is required in a specific application.

An approach gives a strategy and device to discourage unauthorized utilize of a record by the application of a program on a computer framework which takes an advanced picture of an individual and which partners the picture with a database and record data concerning such individual is displayed in [33]. The reference to the record is coded on the card utilizing symbology or coding associated to a chip or attractive medium on or something else embedded inside the card. When the record is shown for confirmation, the record is connected to a recognizing component the symbology or coding is deciphered, the database is questioned, the specific picture record related with the record distinguished, and the enlistment picture is appeared or printed. An extra the objective of the display approach is to supply a technique and gadget to anticipate the unauthorized utilization of a record by the application of a computer program on a computer framework which takes a computerized picture of a person which is at that point encoded utilizing distinctive calculations into symbology and associated to a report by the printing or other application. When the archive is displayed for confirmation, the symbology is checked and decoded utilizing distinctive calculations to remake and appear or print the enlistment picture. Be that as it may, this approach may take as well much time amid the comparison prepare.

An approach gives a security record and a strategy and device for printing and confirming those archives is displayed in [34]. These reports such as distinguishing proof and credit cards, bundling, names and hangtags, title and information plates, as well as articles printed on papers, foils, and/or plastic sheets and frequently regarded as records. This approach comprises an archive security highlight that is printed onto a print surface of a record and which is considered intangible to the unaided eye. The document security highlight incorporates an essential design/background design printed in one color and at smallest one additional design/background design printed in a moment color and superimposed on the essential design/background design. The designs are outlined not to be reproducible by copiers or scanners but can be recognized in a unique archive with the assistance of a location apparatus such as an optical scanner, with or without a programmed nourish of archives, related to a computer running program that distinguishes and shows the nearness or nonattendance of the security pictures.

An approach for segregation the inkjet-printed fakes and includes extraction strategy of goad marks are delivered in [35]. Goad marks are apparatus marks shaped on a printout by paper transport gears of inkjet printers, and it the noteworthy highlights of inkjet printed materials but it is not so simple to identify it since ink discourages it. Goad marks were visualized and clearly recognized from the

foundation by infrared angled lighting and angle picture preparing. By identifying the presence of goad marks on printouts, segregation of inkjet printed material was accomplished. Within the proposed strategy, goad marks were clearly recognized from the foundation. Subsequently, programmed goad stamp location will be realized, and this rule will moreover be pertinent to sensors for identifying fakes. Subsequently, agreeing to the authors saying, the comes about are critical not as it were for fake discovery but moreover within the field of measurable archive examination.

A coordinate's print-based confirmation and security procedure for profitable archives and items, utilizing moiré escalated profiles is proposed in [36]. This procedure combines our know-how and involvement in a few profoundly specialized spaces: The joining of miniaturized scale content or any other aesthetic microstructure into a black-and-white or color halftone picture (a portrait, a scene, etc.) that is printed on the report; confirmation by implies of more escalated profiles which clearly uncover this microstructure (be it plain or undercover) and make it obvious to the unaided eye. Of course, each of these procedures can be utilized as a free security highlight on its claim, but the combination of all or at slightest a few of them together within the same security component makes the strategy greatly strong and troublesome to fake.

A strategy gives security documents which have numerous areas or zones each of which contains data that is noticeable in more than one way is displayed in [37]. For occasion, one field can contain an outwardly distinguishable picture and a computerized watermark that can be recognized when the picture is checked and handled, another field can contain machine-readable OCR content that can be examined by both a human and by a modified computer, and still another field can contain watermark data which can be connected to the yield of a unique finger impression per-user or gadget which locks a user's iris. The computerized watermark is the result of information that is outwardly discernible to a client of the document and information that's covered up, in this way the report cannot be a extortion by supplanting one component (such as an picture) with a comparative component from another record. The framework combines the advanced information is at that point sent to a printing motor and the ultimate archive is delivered. The computerized watermark is the result of information that is outwardly discernible to a client of the document and information that's covered up, in this way the report cannot be extortion by supplanting one component (such as a picture) with a comparative component from another record. The framework combines the advanced information is at that point sent to a printing motor and the ultimate archive is delivered.

A programmed approval framework of the show strategy peruses different areas on the report, and it too naturally identifies data approximately the client, the distinctive data is associated to approve the record. In any case, the strategy causes more overhead in term of the computational process. A scheme for the secure encryption, enrollment, confirmation, decoding of biometric and true to life distinguishing proof data that can be utilized for distinguishing archives such as E-Passports, E-Identity Card, Driving Licenses (DL), and Credit/Debit/ATM Cards) is displayed in [38]. The special arrangement of steps and the utilize of a combination of obvious watermarking, undetectable delicate watermarking interpreting, invisible-robust extraction, and translating watermarking and encryption deliver diverse layers of assurance with biometrics-based keys and make it essentially incomprehensible for the information to be modified with. This information and the encryption keys are put away in two places: an RF-ID chip implanted into the have media and, through secure channels, a centralized database open as it were by authorized issuing specialists. Subsequently, it is so troublesome for programmers, psychological militants, and unauthorized clients to get to any valuable biometric information and mishandle it. By making the converse grouping of steps are taken after for distinguishing proof, confirmation, and modify location

A strategy of making a moved forward security distinguishing proof archive incorporates the steps of shaping a contactless communication embed unit by electrically interfacing and coordinates circuit counting a chip, a controller, a memory unit, a radio recurrence input/output gadget and a radio wire is displayed in [39]. The contactless insert unit alluded to as a covered substrate counting a central preparing unit ideally within the shape of a chip counting memory, an information input/output gadget and a radio wire are given on a suitable substrate. This unit stores the data and biometrics of the individual as input, that can be embeddings the information and filtering the biometrics by recording gadgets such as a camera for checking a confront, retina, ear, etc. or a palm or unique mark scanner depicted over or any other sensible biometrics information input gadget.

IV. CONCLUSIONS

Identities documents represent a large amount of information supports used nowadays due to the fact that they contain critical data. Even though official documents are secured with techniques such as printed patterns or watermarks; etc, but they still suffer from a lack of security. However, the rich availability of cheap scanning and printing hardware allows non-experts to easily create fake documents that received unprecedented attention by the research community due to its direct connection with dangerous crimes and threats – illegal immigration, financial fraud, human and drug smuggling, terrorism, etc. The quick improvement of network technologies helps hackers to effectively get advanced quality fake IDs via different Web sites, and this opened doors widely for fake IDs markets [40][41]. Some reports indicate that 60% of fake documents can be recognized through detection machines or strategies whereas 80% can be identified by human specialists [11]. This demonstrates that numerous fake documents have not however been recognized. Hence, much work ought to be done to upgrade and create efficient fraud detection strategies. The techniques and strategies surveyed and discussed have drawbacks. Therefore, more work in this field is exceedingly needed to moderate the dangers behind these threats. More ID detections strategies must be researched and made available.

V. A TABLE SHOWS AND COMPARES THE RVIEWED TECHNIQUES AND METHODS

Reference	Technique\s	Results	Open Issues/ Future Work
[6]	Forensic Morphing Detector	The accuracies of a decision tree classifier vary from 81.3% to 98%.	More examples of the facial morphing that would have to be covered.
[7]	Copy–Move Forgery Detection (CMFD)	The accuracy was achieved by this system was 87.0% of detecting forgery documents.	The researchers see a need for future research examining the relation between font and block sizes as factors jointly influencing detection performance. They also encourage further research on the development of new (or adjustment of the existing) scanner and paper forensics techniques in order to enable a reliable detection of copied background areas.
[10]	Bounding ox tool	Efficiency of 85.7% was achieved by this system in detecting forgery photocopied documents.	This approach may take too much time during the comparison process. The work under investigation to have a classification based on single approach rather than a hybrid approach to have a better computational efficiency.
[11]	Support Victor Machine (SVM)	Accuracy of whole dataset was 76.75%.	Further enhancement could be achieved by finer segmentation of the printed area aiming to improve noise analysis. Experimenting on documents of different formats (e.g. tabular, graphic) would also be useful for testing the approach.
[15]	Geometric Moments and Gray Level Co-Occurrence Matrix	Efficiency of 94.59% was achieved by the approach in detecting forgery photocopied documents.	This work is under investigation to have a classification based on single approach rather than a hybrid approach to have a better computational efficiency.
[16]	Counterfeit Protection System (CPS)	The accuracy for pattern classification is shown to be up to 93 %. For CPS.	The evaluation would benefit if also the decoding of the patterns other than the Xerox type would be known.
[19]	Counterfeit Protection System (CPS)	Evaluation proved an accuracy of up to 91%.	This system would be more efficient if a technique to reduce the print and scan noise is added.
[20]	Multi-size Block Benford's Law	Experiments conducted over electrophotographic (EP) printers and deskjet printers achieve average of 94.0% efficient.	Development of mixed forensic features for printer model identifications in conjunction with noise features in printed documents should be done.
[21]	Discrete Cosine Transformation (DCT)	Note that the classification accuracy of the DCT feature for the three classes (inkjet, laser and copy) at 400 dpi exceeds 90%.	This approach deals only with a pure text document. It may fail to detect image forgery.
[22]	Steganography	Efficiency of 72.0% was achieved by this system in detecting forgery identity documents.	Steganography's systems require a lot of overhead to hide relatively few bits of data. In the future work for this tool will involve tackling the problem of image compression (below 75%) and how to overcome it.
[23]	Machine Readable Zone (MRZ)	The recognition of this system was 99.8% of detecting forgery documents.	In the future, they will develop an improved module for removing the hologram and extracting the background image from the characters to increase the recognition rate.

REFERENCES

[1] "The hsuduma bill, 2019 arrangement of clauses," 2019.

[2] "Estonian eID scheme : ID card," 2018.

[3] O. Social and S. Card, "Application for a Social Security Card Applying for a Social Security Card is free !," no. 0960, pp. 1–5, 2018.

[4] A. B. Hassan, "A Survey on Techniques of Detecting Identity Documents Forgery," no. 1, 2017.

[5] Onfido, "How to Detect the 7 Types of Document and Identity Fraud Document and identity fraud :," white paper, 2019.

[6] C. Science, C. Kraetzer, and M. Hildebrandt, "Modeling Attacks on Photo-ID Documents and Applying Media Forensics for the Detection of Facial Morphing," pp. 21–32, 2017.

[7] S. Abramova, "Detecting Copy – Move Forgeries in Scanned Text Documents," pp. 1–9, 2016.

[8] L. Rochelle, A. M. Crepeau, and L. Rochelle, "A Conditional Random Field Model for Font Forgery Detection," 2015.

[9] J. Liu-jimenez and R. Sanchez-reillo, "Making Stronger Identity for EU Citizens," pp. 333–339, 2015.

[10] S. V Patgar, "An unsupervised intelligent system to detect fabrication in photocopy document using Variations in Bounding Box Features," pp. 1–6, 2014.

[11] C. Mandridake, A. Ouddan, M. Hoarau, and K. Win-lime, "Towards Fully Automatic ID Document frauds detection," pp. 1–6, 2014.

[12] S. Elkasrawi, "Printer Identification using Supervised Learning for Document Forgery Detection," 2014.

[13] F. C. Sasso, R. Alexandre, R. De Moraes, and J. E. Martina, "A Proposal for an Unified Identity Card for Use in an Academic Federation Environment," 2014.

[14] M. Agarwal, "Smart Ration Card Using RFID and GSM Technique," pp. 485–489, 2014.

[15] S. V Patgar, "An Unsupervised Intelligent System to Detect Fabrication in Photocopy Document using Geometric Moments and Gray Level Co-Occurrence Matrix," vol. 74, no. 12, pp. 29–36, 2013.

[16] T. M. Breuel, "Automatic authentication of color laser print-outs using machine identification codes," pp. 663–678, 2013.

[17] D. Potolinca, I. Sandu, and G. I. Olteanu, "THE STUDY OF DOCUMENTS COUNTERFEIT PROCEDURES," vol. 2, no. 3, pp. 221–233, 2012.

[18] J. Van Beusekom and F. Shafait, "Distortion Measurement for Automatic Document Verification," 2011.

[19] J. Van Beusekom, M. Schreyer, and T. M. Breuel, "Automatic Counterfeit Protection System Code Classification," vol. 7541, pp. 1–8, 2010.

[20] W. Jiang, A. T. S. Ho, H. Treharne, and Y. Q. Shi, "A Novel Multi-size Block Benford ' s Law Scheme for Printer Identification," pp. 643–652, 2010.

[21] C. Schulze, M. Schreyer, A. Stahl, and T. Breuel, "Chapter 7 USING DCT FEATURES FOR PRINTING TECHNIQUE AND COPY DETECTION," pp. 95–106, 2009.

[22] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Combating Digital Document Forgery using New Secure Information Hiding Algorithm," pp. 922–924, 2008.

[23] Y. Kwon and J. Kim, "Recognition based Verification for the Machine Readable Travel Documents."

[24] J. Van Beusekom, F. Shafait, and T. M. Breuel, "Document Signature Using Intrinsic Features for," pp. 47–57, 2008.

[25] P. Vinicius, K. Borges, J. Mayer, and E. Izquierdo, "Document Image Processing for Paper Side Communications," vol. 10, no. 7, pp. 1277–1287, 2008.

[26] A. K. Mikkilineni, P. Chiang, G. N. Ali, G. T. Chiu, J. P. Allebach, and E. J. Delp, "Printer Identification Based on Texture Features," 2005.

[27] P. Classification, "PROCESS FOR PRINTING AFLUORESCENT SECURITY FEATURE ON IDENTIFICATION CARDS AND CARDS PRODUCED THEREFROM," vol. 1, no. 19, 2005.

[28] D. U. Open, "PROTECTION OF IDENTIFICATION DOCUMENTS USING OPEN CRYPTOGRAPHY," vol. 1, no. 19, 2005.

[29] P. Alto, H. Daniel, T. Krivacic, S. Jose, P. E. Williams, and A. E. Singh, "SYSTEMS AND METHODS FOR FORGERY DETECTION AND DETERRENCE OF PRINTED DOCUMENTS," vol. 1, no. 12, 2005.

[30] A. K. Mikkilineni, G. N. Ali, P. Chiang, G. T. C. Chiu, J. P. Allebach, and E. J. Delp, "Signature-Embedding In Printed Documents For Security and Forensic Applications," vol. 5306, no. 0219893, pp. 455–466, 2004.

[31] J. Picard and W. Street, "Digital authentication with copy-detection patterns," vol. 5310, pp. 176–183, 2004.

[32] A. Ag and D.- Leverkusen, "Multifunctional Optical Security Features based on Bacteriorhodopsin," vol. 5310, no. 6421, pp. 117–124, 2004.

[33] P. B. Gardens, P. Examiner, S. Alam, and A. E. Pham, "SYSTEM FOR VERIFICATION AND ASSOCATION OF DOCUMENTS AND DIGITAL IMAGES," vol. 1, no. 12, 2004.

[34] R. U. S. A. Data, "SECURITY DOCUMENTS AND A METHOD AND APPARATUS FOR PRINTING AND AUTHENTICATING SUCH DOCUMENTS," vol. 1, no. 19, 2003.

[35] Y. Akao, K. Kobayashi, S. Sugawara, and Y. Seki, "Discrimination of inkjet printed counterfeits by

spur marks and feature extraction by spatial frequency analysis," vol. 4677, pp. 129–137, 2002.

[36] I. Amidror, "A new print-based security strategy for the protection of valuable documents and products using moire intensity proffles," vol. 4677, pp. 89–100, 2002.

[37] W. Linn, "PRINTING AND VALIDATION OF SELF VALIDATING SECURITY DOCUMENTS," vol. 1, no. 12, 2002.

[38] R. U. S. A. Data, "METHODS AND DEVICES FOR ENROLLMENT AND VERIFICATION OF BIOMETRIC INFORMATION IN IDENTIFICATION DOCUMENTS," vol. 2, no. 12, 2002.

[39] F. M. Chua, P. Examiner, and B. C. Lee, "METHOD OF MAKING AN IMPROVED SECURITY IDENTIFICATION DOCUMENT INCLUDING CONTACTLESS COMMUNICATION INSERT UNIT," no. 19, 2000.

[40] N. Document and F. Unit, "Guidance on examining identity documents 2016," 2016.

[41] N. Document and F. Unit, "Guidance on examining identity documents 2015," 2015.