Computers, Materials & Continua
DOI:10.32604/cmc.2021.014758
Article

Tech Science Press

Hacking Anti-Shoplifting System to Hide Data within Clothes

Al Hussien Seddik Saad[1,*], E. H. Hafez[2] and Zubair Ahmad[3]

[1]Department of Computer Science, Faculty of Science, Minia University, Al-Minya, 61519, Egypt
[2]Department of Mathematics, Faculty of Science, Helwan University, Cairo, Egypt
[3]Department of Statistics, Yazd University, Yazd, Iran
[*]Corresponding Author: Al Hussien Seddik Saad. E-mail: al.hussien_seddik@mu.edu.eg
Received: 14 October 2020; Accepted: 08 November 2020

Abstract: Steganography has been used to prevent unauthorized access to private information during transmission. It is the scheme of securing sensitive information by concealing it within carriers such as digital images, videos, audio, or text. Current steganography methods are working by assigning a cover file then embed the payload within it by making some modifications, creating the stego-file. However, the left traces that are caused by these modifications will make steganalysis algorithms easily detect the hidden payload. Aiming to solve this issue, a novel, highly robust steganography method based on hacking anti-shoplifting systems has proposed to hide data within clothes. The anti-Shoplifting system is an anti-theft security system that protects goods and products, leaving the store in an illegal way (i.e., without paying for them). The proposed method works by modifying the default anti-shoplifting system by changing its built-in soft RFID (radio-frequency identification) tags sewn in clothes into NFC (Near Field Communication) tags. These NFC tags are smart tags that can communicate with NFC-Enabled smart-phones using NDEF (NFC Data Exchange Format). NDEF is one of the advancements added to RFID technology by NFC, which allows the data exchange. Every NDEF message has one/more NDEF records that contain record type, a unique ID, a length, and a payload of data that contains the secret message content that can be any type of data that fits in a byte stream. Based on NDEF and NFC-enabled smart-phones, the proposed method will take the secret message from the sender, make use of his NFC-enabled smart-phone to communicate with the NFC tag, then hide the secret message within the NDEF's payload of the NFC tag stuck in clothes. Finally, to evaluate the proposed method, it has been compared with default (digital) steganography weak points. Such as time, lockable, robustness, attacks, capacity, and a few more points. The results and comparisons showed that the proposed method is more efficient than default (digital) steganography and has many advantages.

Keywords: Near-field communication; radio-frequency identification; Steganography; data hiding; tags

1 Introduction

The development of information technology (IT) and the everyday use of smart-phones have participated in the ever-growing frequency of communication between users in modern society [1]. However, confidential information as passwords, banking account details, private appointments, and personal IDs has leaked through intentional or illegal actions of individuals during data transmission resulting in serious losses. In this case, has required to provide a secure channel between users to protect their sensitive data from leakage attacks like phishing, hijacking, hacking, and cyber-attacks like "man-in-the-middle" (MITM), "message disclosure," and "manipulation by readers" (MBR) [2].

The proposed method has based on the following; Steganography, Anti-shoplifting system-Electronic Article Surveillance (EAS), Near-field communication (NFC) technology, and NFC-Enabled smart-phones. So, the rest of this section will briefly discuss these topics.

1.1 Steganography

Information hiding is a powerful technique that embeds a secret message within a cover of innocent media such as audio, image, text, and video and displays meaningful content so that suspicion is not aroused [2]. So, the required secure communication can be achieved by information hiding [1].

As known, steganography (i.e., information hiding) is a word of Greek origin that means covered writing [3]. It is a strategy in which a secret message is transmitted safely by concealing it in any other carrier in such a way that the carrier does not change significantly and appears the same as the original. So, the goal is to hide the communication itself to raise suspicion [2]. Another definition is "hiding in plain sight," in which the message is "out in the open" but goes undetected. In short, communication is happening in front of someone's eyes, but unless they are the sender or the receiver, the message goes unnoticed [3].

1.1.1 Steganography System Components [3]

The components of the steganography system are:

- Cover or Carrier: Is the host into which the secret message is embedded.
- Secret Message: The confidential message that will be embedded within the carrier.
- Stego-Object: The resultant object that is obtained after embedding the message.
- Embedding Algorithm: Is the method that embeds a secret message within a carrier.
- Extraction Algorithm: The method by which payload has extracted from stego-object.

1.1.2 Steganography System Evaluation Criteria

Many considerations must be taken when designing a steganography system. However, the common criteria are the following [2]:

- Invisibility: Is the ability to be undetected (i.e., payload effect must be invisible) [2].
- Hiding Capacity: Maximum amount of data that can be embedded or extracted correctly [4].
- Robustness: Stego-object resistance to malicious or unintentional changes or attacks [2].
- Security: This measure depends on the three criteria stated above; a technique must provide a balance among these criteria to obtain a higher level of security [2].

1.1.3 Steganography System Attacks

There are three different types of steganography attacks [3]:

- Passive attack: The attacker is just observing the communication without any interference. Therefore, if the attacker cannot modify the stego-object's contents during communication, he is called a "passive attacker" [3].
- Active attack: In this type of attack, the attacker can modify the stego-object's contents during communication [3].
- Malicious Attack: In this attack, the attacker can fake messages or acts as a sender or receiver during the communication process [3].

1.1.4 Coverless Steganography

Traditional data hiding methods work by carrier modifications; these modifications cannot resist steganalysis tools. So, the coverless data hiding concept has been proposed [5]. It does not mean that cover is not required [6], or sensitive data can be transmitted with no cover medium. Instead, the embedding of the payload is achieved by carriers generation or by mapping a secret message with it [7].

It is categorized into text, and image steganography depends on carrier type. In coverless text data hiding, the secret data is embedded by establishing a relation between texts and words; then, this information is embedded according to mapping rules [7]. On the other hand, coverless image data hiding is classified into a generation of images based on the secret message and establishing a mapping rule between the carrier and secret data to represent it [8]. Therefore, this steganography (i.e., coverless) methods have a security level higher than traditional methods [5].

1.2 Anti-Shoplifting System–"Electronic Article Surveillance" (EAS)

The anti-shoplifting system (EAS) is an anti-theft security system that creates a field to protect products and goods, leaving the store in an illegal way. The system consists of an antenna (placed at the entrance of the store as gates, see Fig. 1) and special tags that are attached or sewn into the store's products, see Fig. 2. An alarm will set off if a shoplifting attempts occur [9]. Let us look closely at this technology and discover how it works.

Figure 1: Anti-shoplifting (EAS) gates [10]

1.2.1 Anti-shoplifting Devices

In addition to having a transmitter and receiver (see gates shown in Fig. 1) at the entrance, every product in the store has a concealed RFID tag. In bookstores, soft tags can be found attached to one of the pages inside the book. Also, in clothes stores, as it is the point of research in this paper. There is typically a "hard tag" (round plastic tag) locked onto each item with a sharp metal spike, or "soft tags" that are cleverly concealed within clothes' labels so it cannot be spotted as in Fig. 2 [10].

Figure 2: Anti-shoplifting (EAS) tag/label [10]

So, how is the alarm set off? If you walk through the gates without paying for something, the radio waves transmitted from the transmitter that is hidden in on one of the gates are picked up by the tag's coiled metal antenna that is concealed in the clothes label. This, in turn, generates an electrical current, which makes the tag broadcast a new radio signal of its own at a specific frequency. Then the other gate that contains the receiver picks up the new radio signal that is transmitted by the tag and set off the alarm.

Why does not the alarm sound after paying for something? After paying the checkout, the checkout assistant deactivates the item's tag by passing it over or through a deactivating device. This, in turn, destroys/deactivates RFID tag electronic components so they will not transmit a signal when walking through the gates, and the alarm will not set off [10].

1.2.2 RFID Tag

RFID is not a technology for communications; instead, it is designed for identification purposes. "Radio-Frequency Identification" is a technology which interchanges information between transmitter and receiver [11].

The great potentiality of RFID is because the transmitter is an electronic label, called a tag that is thin enough to be molded in any shape [12]. From tap-and-go payment to the tags sewn into consumer products such as clothing labels to deter theft (anti-shoplifting), most of us encounter RFID tags a few times a week [11].

1.3 NFC

Near Field Communication can be defined as the technology of short-range wireless communication, which has been developed by "Philips" and "Sony" by the end of 2002 for contactless communications [13]. NFC is a data transmission system that uses the technology of RFID. It is a short-range and high frequency (13.56 MHz) technology that allows devices to exchange data between them. The primary feature of NFC comes from the very short distance allowed

between devices to communicate, which must be few centimeters (maximum distance is around 5 cm) [14,15]. This very short distance has significant advantages such as a greater level of security with regards to eavesdropping and a very short interval of time to set up a connection (it takes about "tenth of a second" to set up a connection) [16].

1.3.1 NFC-Enabled Smart-Phones

Smart-phone technology continues to grow with the addition of new features that make this tool multi-use. One of the most important features that have been embedded in smart-phones is NFC. NFC allows the smart-phone to be offline communicate with other NFC-enabled smart-phones without going over any network at a distance of few centimeters (i.e., offline data transfer). Besides, NFC-enabled smart-phones can also read data stored in smart cards and NFC tags. Currently, almost all smart-phone devices are equipped with NFC. In 2018 about 1,907 million smartphones were NFC-enabled [17].

NFC technology facilitates the usage of smart-phone for people by offering many services such as payment applications, access controls for offices and houses, among others. Finally, the technology of NFC integrates all of these services into the smart-phone [15].

The first "NFC-enabled smart-phone" was introduced in 2006 by Nokia, but the commercial interest in "NFC-enabled smart-phones" became famous in 2010 after Samsung produced the Nexus S smart-phone [18]. The integration of NFC into smart-phone has further opened up opportunities for new applications or business models [19].

1.3.2 NFC Tags

NFC tags consist of the following components; an antenna and a small amount of memory, see Fig. 3. These tags do not have a built-in power source, and they take power for transferring data from other devices such as NFC-enabled smart-phone or NFC readers [16].

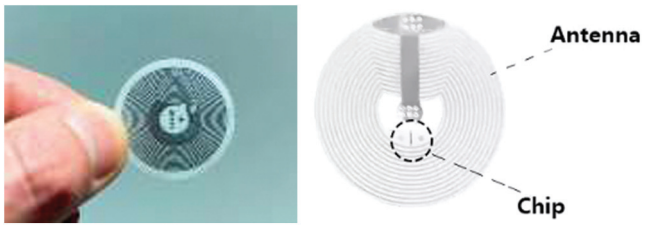

Figure 3: Example of an NFC tag [16]

Blank NFC tags can hold any type of data. These tags are tiny in size, about 2 square centimeters in area. So, it can be integrated within any object easily without making any noticeable changes [16].

1.3.3 NDEF

Data is formatted using the NDEF that allows data exchange between NFC tags and devices. NDEF is one of the advancements that added to RFID technology by NFC [11].

NDEF is a standard data format that operates across all NFC devices, regardless of the tag or device technology. Every NDEF message has one/more NDEF records. Each record is made up of a header and a payload, see Fig. 4a [11].

The header contains metadata about the record, such as a particular record type, a unique ID, a length, and so forth, see Fig. 4b, and the payload contains the content of the message that can be any type of data that fits in a byte stream [11].

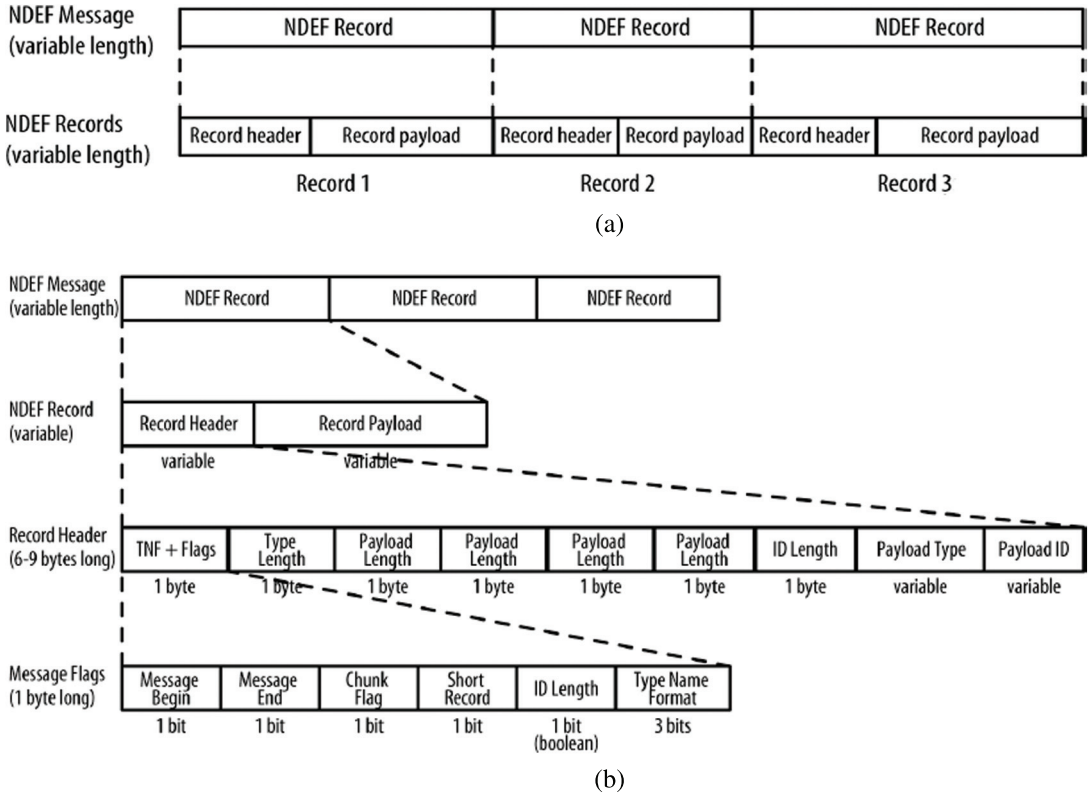

Figure 4: (a) NDEF message that contains several records [11] (b) The structure of the NDEF message, with details about the header [11]

As shown in Fig. 4b, an NDEF record consists of a TNF (type name format), a payload type, payload ID (identifier), and the payload (i.e., the content you are transmitting). The TNF tells how to interpret the payload type. The payload type is a MIME (Multipurpose Internet Mail Extensions) media type, NFC-specific type, or URI (Uniform Resource Identifier) that tells how to interpret the payload. So, TNF is the metadata about the payload type, and the payload type is the metadata about the payload. The payload ID is optional and allows multiple payloads to be cross-referenced [11].

NDEF library does not care what the payload is; it just passes it on (i.e., It can be plain or encrypted text, binary, or anything else). It depends on the applications to agree on the payload format and type [11].

NFC transactions are generally short. Each exchange generally consists of only one message, and each tag carries just one message [11].

1.3.4 NFC vs. RFID

NFC is compatible with the existing infrastructure of RFID technology, and they are often conflated, but they are not the same [13]. Though NFC readers are able to read from or write to some RFID tags, NFC has more capabilities than RFID and enables a more excellent range of uses. NFC can be considered an extension of RFID, built on some RFID standards to create a broader platform for data exchanging [11].

1.3.5 NFC Interaction Styles and Operating Modes

NFC communication is taking place between two compatible NFC devices near located to each other using the operating frequency stated before, which is 13.56 MHz; it provides easy communication between various NFC devices with transfer rates of 106, 212, and 424 Kb/s. The initiator device is the one that starts the communication, while the respondent one is called the target [13].

As known, "NFC-enabled smart-phones" and NFC readers use their own built-in power. Hence they are active devices, whereas an NFC tag uses their power, so it can be called a passive device. Almost all initiators are active devices; however, the target device can be passive/active, depending on its operating mode [13].

NFC protocol is occurring using two modes of communication, which are passive mode and active mode. In an active mode of communication, both devices use their own built-in power to generate their RF field to allow data transmission. While in the passive mode of communication, the RF field is generated only by the initiator, and the target device uses the already created energy [13].

Three types of NFC devices that are involved in NFC communication. NFC-enabled smart-phones, NFC readers, and NFC tags. The possible interaction among these devices provides three distinct modes for the operation, which are; "reader or writer," "peer-to-peer," and "card emulation" mode [13].

- "Reader/Writer" Operating Mode: Communication will be initiated by an NFC-enabled smart-phone (active device), and it can either read from/write to an NFC tag (passive device) [13].
- "Peer-to-Peer" Operating Mode: A bidirectional connection between two NFC-enabled smart-phones will be established. In this mode, NFC-enabled smart-phones have the ability to exchange any type of data [13].
- "Card Emulation" Operating Mode: The user makes the NFC-enabled smart-phone touch an NFC reader; in this case, the NFC-enabled smart-phone behaves like an ordinary smart card [13].

1.3.6 NFC Advantages [14]

- Security: Communication between NFC devices are limited to a distance that is lower than five centimeters. It starts by bringing two NFC devices very near to each other and terminated immediately by separating the devices beyond a specific limit [13], this, in turn, forcing the receiver to be physically located in the required location [14].
- Cost: NFC tags are a low-cost technology, and its implementation is cheap [14]. It can be found in the market online for a price starting from 0.05 $ per unit.
- Compatibility: Almost all smart-phones and tablets are currently incorporating NFC as a built-in feature (i.e., no special devices required to read/write NFC tags) [14].

Finally, the main contributions of this paper are; proposing a novel steganography technique that ensures the security of the secret message and protects confidential information by embedding the message in innocent cover–clothes, which is used as a carrier. Then, developing an android application based on the proposed technique. Finally, a system evaluation will be made by conducting practical experiments.

The organization of this paper will be in this way; Section 2 presents some studies and related works on NFC. Then, Section 3 introduces the proposed method in detail. Next, in Section 4, the proposed method will be evaluated and compared with existing steganography techniques. Finally, Section 5 has the conclusion of the paper.

2 Related Studies

This section surveys some studies and related works on NFC and its applications.

Reference [19] shows a "two-factor authentication access control system" based on an NFC-enabled smart-phone using an encrypted graphical password and a digital key. The system allows users to make use of a digital key, which is stored in their "NFC-enabled smart-phone" to obtain access to premises securely.

Using the NFC-enabled smart-phone instead of the smart card is more secure, but the phone has to be charged all the time, and there is no way to be switched off; otherwise, access will not be granted to the user.

Also, a way to unlock NFC-enabled smart-phones by using NFC-enabled tattoos has been introduced [16]. The proposed method uses the integrated phone's NFC to unlock itself by tapping it to a digital tattoo stuck onto a user's arm. Each tattoo contains a code that is when detected by the phone unlocks itself. The authors also said that the tattoo would be adhered to a user's skin using a high-quality adhesive. Moreover, the authors stated that each tattoo could live no more than five days, and after this period, the tattoo will be replaced with a new tattoo.

First, the tattoo that the authors talked about is just an NFC tag. Then the authors said that this tag would be stuck on the user's skin using a high-quality adhesive, and this is not a practical solution and also not a secure way to keep a phone password. Finally, the authors decided that the life of the tag is only five days; why?

Moreover, a solution to detect Drug–Drug Interactions based on NFC technology has been presented [20]. The proposed method works as follows: NFC tags will be attached to drug containers and encoded by the drug suppliers. Then, drugs are scanned to reveal any possible drug interactions. Then the authors introduced the proposed system, which consists of two parts; the Pharmacy Terminal, where the information will be encoded in NFC tags, and the Patient Terminal, where those drugs will be scanned. The authors also said that the tags would be encoded using a special device connected to a local database, and this software is connected to an NFC Reader or Writer that does the encoding of NFC tags. While in the Patient Terminal, there will be a device comprised of an NFC reader, microcontroller, small screen, and some buttons, and this device will be purchased by the patient. Finally, the authors asked for a unique ID for every drug to be used.

Honestly, the proposed method is theoretically useful, but practically it is too costly for both sides due to all of these hardware components required. This problem can be solved by using "NFC-enabled smart-phone" instead of using all of these devices and hardware components that

the authors introduced, and it will do all the work. Finally, users are asked to use a unique ID for every drug. Actually, the NFC tag already has UID that can be easily used.

Furthermore, an android application that is based on its smart-phone integrated NFC has been proposed [21] to emulate as an NFC card through "Host Card Emulation" (HCE) that manages the passcodes instead of pressing the keypad in any access control system. The authors also limited the number of passcode digits to 4 digits only.

The proposed method looks similar to the access control system [19]. However, in this method, the authors limited the passcode into four digits only without saying the reason. This reduces security, as four digits have a too-small number of combinations that can be cracked easily.

As well, an NFC-based "electronic medical record" (EMR) application has been developed [17]. The proposed application on the doctor's phone can read/change the electronic medical record, while on the patients phone can be used for reading only. When the patient visits the doctor for the first time, EMR needs to be copied from the patient's phone by a tap between both phones. The proposed application is handy for both doctors and patients as it saves time for them.

Additionally, a student sign-in application for classrooms and educational centers has been introduced [14]. The system works as follows: every classroom will be equipped with an active NFC device or an NFC tag through which students bring their NFC-enabled smart-phones close enough to sign-in. So, students can sign-in correctly by bringing their smart-phones, with the application installed, close to an NFC tag, following the "Tap & Go" mode. The proposed system is an effective sign-in system that will save time and organize the process.

Finally, a ticketing system framework for the Croatian ferry lines that depend on using NFC technology has been presented [18] that helps users avoiding geographical and time constraints. The primary advantage of this ticketing system is to manage tickets electronically and avoid losing time found in classical ticketing systems.

This section introduced some NFC-based methods. An authentication access control system and NFC- unlocking tattoos have been introduced. Also, Drug–Drug Interactions and host card emulation have been presented. Moreover, electronic medical records (EMR), student sign-in application, and a ticketing system framework have been defined. The next section is going to make use of NFC technology differently; it is going to use it as a secure carrier for secret messages (i.e., hard-cover).

3 Proposed Method

To transmit private information securely and to be protected from the above-stated attacks, a motivating scenario will be presented to explain the research challenge of the proposed method.

Suppose that two users X and Y are sensitive users working with any message transmission application such as "short message service" (SMS), social media applications, or even E-mails to exchange this sensitive information. The problem is that; this sensitive information can be accessed by a MITM attacker as he may be eavesdropping on this transmission, and if he succeeded, a "Message disclosure attack" (i.e., information leakage) or "manipulation by reader" (MBR) attack would happen. Another problem is that provider of the service has permission to access transmitted messages as these messages are already stored in his database servers [2]. Even if steganography (i.e., data hiding) has been used, digital cover files such as video, audio, digital images, and text are of very low robustness to resist manipulations and modifications,

intentionally/unintentionally. So, sensitive information will be lost, modified, or tampered with during transmission.

Thus, it is obvious that a safe and secure message transmission/hiding technique is required to stand against these attacks and challenges. So, to address the problem, a new steganography technique that is based on hacking an anti-shoplifting system to hide data within clothes using NFC tags has been proposed.

The proposed method consists of two main sides: the sender/embedding side, where the sender uses his NFC-enabled smart-phone to hide the secret message within a selected piece of cover-clothes to create a stego-clothes, and the receiver/extraction side, where the receiver extract the secret message from the stego-clothes.

Before discussing both sender and receiver sides in detail, the proposed steganography system components will be introduced next.

3.1 Proposed Method Components

- Cover–Clothes (Carrier): The clothes that contain a soft NFC tag, into which payload is embedded.
- Secret message: The sensitive message that will be embedded within the NFC tag added to the clothes.
- Stego-Clothes: Clothes were obtained after embedding the secret message within an NFC tag.
- Embedding Algorithm: The algorithm that embeds the secret message within a clothes' NFC tag.
- Extraction Algorithm: The algorithm by which a secret message is extracted from the clothes' NFC tag.

3.2 The Sender or Embedding Side (Fig. 5)

- The sender will choose a store that has an anti-shoplifting system with soft tags.
- Choose any cover-clothes with a soft RFID tag.
- Replace the soft RFID tag with an NFC (or just stick a new NFC sticker above the clothes label).
- Run the proposed application on an NFC-enabled smart-phone to write the secret message on it.
- Embeds the secret message within the cover-clothes label to create stego-clothes, "tap & Go" mode.

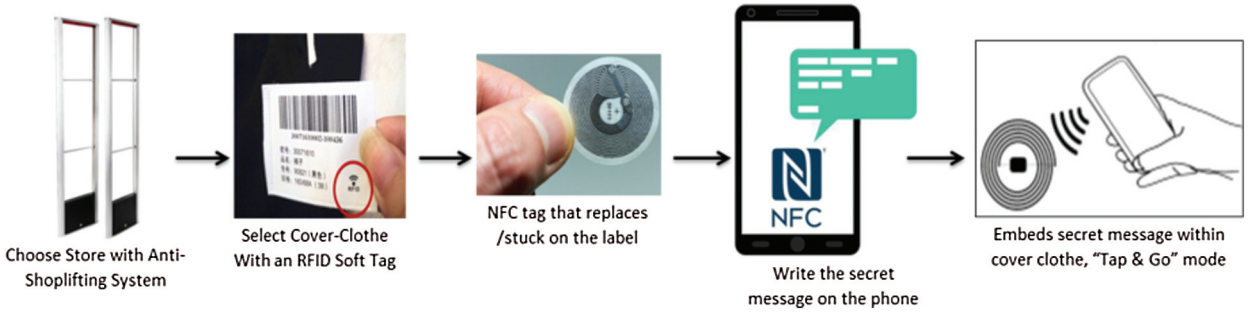

Figure 5: Sender/embedding side

3.3 The Receiver/Extraction Side (Fig. 6)

- The receiver has to go to the same store.
- Select the same stego-clothes that the sender used.
- Run the proposed application on his NFC-enabled smart-phone.
- Tap the phone over the stego-clothes label.
- Extract the message from the stego-clothes.

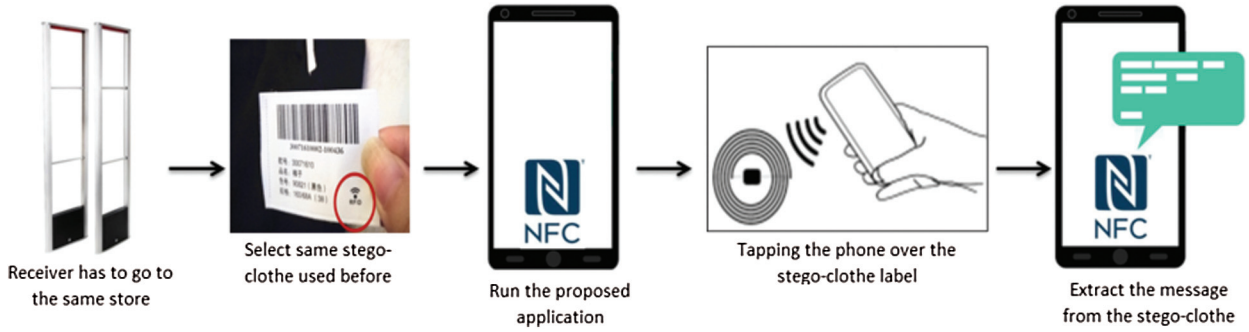

Figure 6: Receiver/extraction side

To this point, the first contribution of this research has been achieved, which is proposing a novel steganography method that hides and protects sensitive user information by embedding the secret message in innocent cover-clothes, which is used as a carrier to create a stego-clothes.

The second and third contributions, which were developing an android application based on the proposed steganography method and evaluating the system by conducting practical experiments, will be discussed next.

4 Evaluation and Comparisons

In this section, the method's application will be introduced, and the proposed method will be tested, compared, and evaluated. The proposed method's application has been implemented in Java programming (Android studio 4.0.1), see Algorithm 1, and the experiments executed on various "NFC-enabled smart-phones" with Android OS.

NFC tag sticker used in the proposed system can be found online here [22], and it has the following specifications:

- Adhesive: Wet Glue.
- Writable: 10000 times.
- Reading Distance: Max. 50 mm.
- Basing Material: Paper.
- Size: Round 25 mm.
- Thickness: 0.2 mm.
- Smartphone Compatibility: Yes.
- NDEF: Full compliance with the NDEF NFC.
- Capacity: 144 bytes of R/W memory area.
- Lockable: Yes (can be made to read-only).

Algorithm 1: Secret message embedding

Input: Secret Message (SM).

```
grant NFC Permission                    // Android–manifest.xml: "android.permission.NFC".
grant NFC Feature;                      // Android–manifest.xml: "android.hardware.nfc".
  If (phone is NFC-enabled smart phone)  // Checking Phone.
      if(NFC is Active)                  // Checking NFC state, If Enabled.
          Set phone to auto-detect NFC tags;  // Android—Enable Foreground Dispatch.
          if(NFC Tag Detected)           // Phone detects an NFC tag.
            If (NDEF of tag! = null)     // Tag is formatted.
              Write SM into NFC Tag      // Embed Secret Message into an NFC tag.
              goto step 6;               // go to step 6, Check if another tag is detected.
            else                         // if ndef of the tag == null → needs formatting.
              Format Tag;                // Format tag to be able to write on it.
              goto step 7;               // go to step 7, Check if NDEF of the tag still null
            end if
          else                           // if no NFC tag is detected.
            goto step 6;                 // go to step 6, Check again.
          end if
      else                               // Checking NFC state, If Disabled.
          Display ("Please Enable NFC"); // Display Message to enable phone's NFC
          goto step 4;                   // go to step 6, Check again
      end if
else                                     // if the phone is not NFC-Enabled
      Display ("Phone isn't Supporting NFC")  // Display Message to user
end if
end
```

Also, in [23], an up-to-date list of all NFC-enabled smart-phones and their compatibility with NFC Chips'.

4.1 Evaluation Criteria Analysis

For evaluation purposes, the proposed method's application has been tested multiple times in different real-life situations. The application is working as intended and hides/extracts messages every time after touching the clothes. In this subsection, we evaluate the proposed method based on the evaluation criteria discussed before.

- Embedding Capacity: Since the embedding algorithm hides message within NFC tags, the embedding capacity depends on tag type. Multiple tags can be used at the same time. The sender can divide his secret message on more than one piece of clothes. So, the whole store can be used.
- Invisibility: Invisibility means that the effect of a payload in the carrier must be invisible. As discussed before, the secret message will be embedded within the label of the cover-clothes to create the stego-clothes. So, the clothes themselves will not be changed or modified. Also, the NFC tag will not be changed or modified. So, there will not be any detectable changes, and both the clothes and the tag will be identical.

- Robustness: As defined above, it is the resistance to changes/attacks; In fact, NFC tags are not like digital cover files that can be manipulated or changed. Also, it is not connected to any network (offline), so it is also protected from hacking. NFC tags can only be written by an "NFC-enabled smart-phone," This problem can be solved by locking the tag after writing the required secret message. Once it is locked, the written secret message cannot be modified or deleted.
- Security: Since the method provides optimum balance between other criteria-higher embedding capacity, high invisibility, and high robustness, it is able to secure the secret message perfectly. Also, since the secret message is not transmitted over the internet, cellular networks, or stored on servers and the proposed method works in an offline mode, the steganography attacks stated above is very hard or impossible to occur.

4.2 Comparison Results

The proposed clothes steganography will be compared to traditional steganography and coverless steganography methods; to evaluate the efficiency, security, flexibility, facility, and time of the proposed method.

Tab. 1 compared NFC steganography and traditional steganography in some points. The first point is the carrier; in NFC steganography, the carrier is a hard cover (i.e., NFC tag). So it cannot be affected by viruses, attacked, manipulated, or modified like soft covers (i.e., images, audio, and text).

Table 1: Characteristics comparison between traditional steganography and NFC steganography

	Digital steganography	Clothes steganography
Carrier	Digital cover file [24].	Cover–clothes (NFC tag).
Secret data	Payload [24].	Payload.
Files	At least two files [24].	No files are required.
Output	Stego-file [24].	Stego-clothes.
Flexibility	No, limited to digital covers [24].	Yes, a tag can be hidden in any object.
Fails when	Detected [24].	Tag destroyed.
Visibility	Never [25].	Yes/no (it is a label, not suspicious).
Type of attack	Steganalysis [25].	No attacks.
System is invalid if	Detected/aroused suspicion [26].	–
Robustness (attack)	Very low.	Very high (as discussed above).
Robustness (manipulation)	Very low.	Very high (as discussed above).
Independent of file format	No.	No files are required.
Timing requirement	Depends on cover and payload.	About a tenth of a second [16].
Lockable	No.	Yes (can be read-only) [22].
Cover/stego file similarity	Similar to somehow.	Identical (as it is a hardware chip).

The files are another comparison point; in traditional steganography, at least two files are required, cover file and stego-file. This file requires an internet connection (i.e., an insecure channel) to be transmitted to the receiver. While in NFC steganography, no files are required, no connection is needed, and there is no transmission process. One more point is the output, which faces the same issues as it is a file.

Next is flexibility; in traditional steganography, there is no flexibility as only digital covers can be used. While in NFC steganography, the NFC tag can be hidden or stuck in any object like books, clothes, watches, laptops, food packs, etc.

Fails when; traditional steganography fails when a stego file is detected, modified, deleted, or attacked. In contrast, NFC fails when the tag is destroyed, as it cannot be detected because it is hidden within an object (clothes in our case).

Also, visibility is a comparison point. Traditional steganography cannot be visible. If it can be seen, then the algorithm fails. While in NFC, it is only a clothes' soft tag, and it is visible to all.

The attack is an important comparison point. Traditional steganography is attacked by MITM, MBR, steganalysis, modifications, and manipulations. In contrast, NFC steganography is not susceptible to these attacks, as it is a hard cover.

Robustness is very high in NFC steganography, as no modifications or manipulations can be done to the tag. Another problem is the file format; not all formats can be used in traditional steganography, such as jpeg images or any files that are lossy compressed as the secret message will be lost.

The timing factor also is a vital comparison point. In traditional steganography, it depends on hardware specifications, secret message size, and cover size. In NFC, it takes only a tenth of a second to embed a full-length secret message.

Lockable is a unique advantage of NFC steganography. NFC tag can be locked (i.e., to be read-only) to be protected from data modifications. Finally, the cover file and stego file are not the same, not identical. While in NFC, the tag is the same before and after embedding a secret message.

So, as shown in Tab. 1, after comparing both methods, it has been found that the proposed method is more efficient than digital steganography.

As shown in Tab. 2, the proposed method has the highest hiding capacity among existing coverless steganography methods, 1,152 bits.

Table 2: Capacity comparison between coverless steganography and NFC steganography

Method	Capacity (bits/carrier)
Zhou et al. [27]	8
Yuan et al. [28]	8
Zhang et al. [7]	1∼15
Zhou et al. [29]	16
Zheng et al. [8]	18
Cao et al. [6]	36
Cao et al. [30]	68
Zou et al. [5]	80
Zhou et al. [31]	384
Cao et al. [32]	896
Proposed method	144 bytes $\times$ 8 = 1,152

5 Conclusion

The proposed work extends the boundaries of data hiding capabilities. That is, by creating a new and secure data hiding method within clothes and enabling users to hide/extract or transmit messages securely using their "NFC-enabled smart-phone" as a key to access the NFC tag. The proposed method is able to hide secret information within cover-clothes so that the embedding trace is totally invisible to viewers (as in coverless steganography methods). Also, being an offline data hiding method keeps it perfectly secure against attacks as no internet connection or cellular networks required. Moreover, the analysis of the proposed method confirms that it is able to prevent various attacks. Furthermore, it provides higher embedding capacity, as shown in Tab. 2. This capacity can be enlarged as the user is not limited to a digital cover file; the whole store can be treated as a carrier. Besides, the invisibility of the proposed method is achieved, as the cover-clothes and the stego-clothes are identical. Moreover, robustness is very high, as the payload is not hidden in a digital cover to be modified or attacked. Besides, the proposed method is highly secured as it provides optimum trade-offs between evaluation criteria, offering a high level of safety for the hidden secret message. Finally, since no internet connection, cellular networks, or database servers used in the proposed method, the proposed steganography method is protected from attacks stated above.

Funding Statement: The author(s) received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] H. H. Liu and C. M. Lee, "High-capacity reversible image steganography based on pixel value ordering," *EURASIP Journal on Image and Video Processing*, vol. 2019, no. 1, pp. 1062, 2019.

[2] M. Taleby Ahvanooey, Q. Li, J. Hou, H. Dana Mazraeh and J. Zhang, "AITSteg: An innovative text steganography technique for hidden transmission of text message via social media," *IEEE Access*, vol. 6, pp. 65981–65995, 2018.

[3] N. Dey, A. Ashour and S. Acharjee, *Applied Video Processing in Surveillance and Monitoring Systems*, vol. i, Hershey, Pennsylvania, USA: IGI Global, 2016.

[4] S. Mukherjee, S. Roy and G. Sanyal, "Image steganography using mid position value technique," *Procedia Computer Science*, vol. 132, pp. 461–468, 2018.

[5] L. Zou, J. Sun, M. Gao, W. Wan and B. B. Gupta, "A novel coverless information hiding method based on the average pixel value of the sub-images," *Multimedia Tools and Applications*, vol. 78, no. 7, pp. 7965–7980, 2019.

[6] Y. Cao, Z. Zhou, X. Sun and C. Gao, "Coverless information hiding based on the molecular structure images of material," *Computers, Materials & Continua*, vol. 54, no. 2, pp. 197–207, 2018.

[7] X. Zhang, F. Peng and M. Long, "Robust coverless image steganography based on DCT and LDA topic classification," *IEEE Transactions on Multimedia*, vol. 20, no. 12, pp. 3223–3238, 2018.

[8] S. Zheng, L. Wang, B. Ling and D. Hu, "Coverless information hiding based on robust image hashing," *Int. Conf. on Intelligent Computing*, Liverpool, United Kingdom, vol. 1, pp. 536–547, 2017.

[9] Anti-Shoplifting Systems—EAS. [Online]. Available: https://www.milestone.co.za/product/anti-shoplifting/.

[10] Radio frequency (RF and RFID) tags. [Online]. Available: https://www.explainthatstuff.com/rfid.html.

[11] D. Coleman, B. Jepson and D. Coleman, *Beginning NFC: Near Field Communication with Arduino, Android, and Phonegap*. 1005 Gravenstein Highway North, Sebastopol, CA: O' Reilly Media, Inc., 2014.

[12] A. D. Mastio, R. Caldelli, M. Casini and M. Manetti, "SMARTVINO project: When wine can benefit from ICT," *Wine Economics and Policy*, vol. 5, no. 2, pp. 142–149, 2016.

[13] V. Coskun, B. Ozdenizci and K. Ok, "The survey on near field communication," *Sensors*, vol. 15, no. 6, pp. 13348–13405, 2015.

[14] M. J. L. Fernández, J. G. Fernández, S. R. Aguilar, B. S. Selvi and R. G. Crespo, "Control of attendance applied in higher education through mobile NFC technologies," *Expert Systems with Applications*, vol. 40, no. 11, pp. 4478–4489, 2013.

[15] V. Coskun, B. Ozdenizci and K. Ok, "A survey on near field communication (NFC) technology," *Wireless Personal Communications*, vol. 71, no. 3, pp. 2259–2294, 2013.

[16] U. Jambusaria, N. Katwala and D. Mistry, "Secure smart-phone unlocking using NFC," *Procedia Computer Science*, vol. 45, no. C, pp. 465–469, 2015.

[17] N. C. Basjaruddin, E. Rakhman, K. Kuspriyanto and M. B. Renardi, "NFC based electronic medical record," *International Journal of Interactive Mobile Technologies*, vol. 13, no. 3, pp. 4, 2019.

[18] D. Zupanovic, "Implementation model for near field communication in Croatian ferry ticketing system," *Procedia Engineering*, vol. 100, pp. 1396–1404, 2015.

[19] S. N. Cheong, H. C. Ling and P. L. Teh, "Secure encrypted steganography graphical password scheme for near field communication smart-phone access control system," *Expert Systems with Applications*, vol. 41, no. 7, pp. 3561–3568, 2014.

[20] A. B. H. Altaweel, L. Abusalah and D. M. Qato, "Near field communication detection system for drug–drug interactions," *Procedia Computer Science*, vol. 140, pp. 314–323, 2018.

[21] C. D. Chin and W. Benjapolakul, "NFC-enabled android smart-phone application development to hide 4 digits passcode for access control system," *Procedia Computer Science*, vol. 86, pp. 429–432, 2016.

[22] Buy NFC Tags—Ntag213. [Online]. Available: https://www.alibaba.com.

[23] NFC Compatibility—The up-to-date List of all NFC-enabled Smartphones and Tablets. [Online]. Available: https://www.shopnfc.com/en/content/7-nfc-compatibility.

[24] A. Soni, J. Jain and R. Roshan, "Image steganography using discrete fractional fourier transform," in *Int. Conf. on Intelligent Systems and Signal Processing*, United States, pp. 97–100, 2013.

[25] S. Almuhammadi and A. Al-shaaby, "A survey on recent approaches combining cryptography and steganography," *Computer Science and Information Technology*, pp. 63–74, 2017.

[26] I. Jawad, P. Premaratne, P. James and B. Halloran, "Neurocomputing comprehensive survey of image steganography: Techniques, evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, 2019.

[27] Z. Zhou, H. Sun, R. Harit, X. Chen and X. Sun, "Coverless image steganography without embedding," in *Int. Conf. on Computational Science*, Monte Carlo Resort, Las Vegas, Nevada, USA, vol. 1, pp. 123–132, 2015.

[28] C. Yuan, Z. Xia and X. M. Sun, "Coverless image steganography based on SIFT and BOF," *Journal of Internet Technology*, vol. 18, pp. 435–442, 2017.

[29] Z. L. Zhou, Y. Cao and X. M. Sun, "Coverless information hiding based on bag-of-words model of image," *Journal of Applied Sciences*, vol. 34, pp. 527–536, 2016.

[30] Y. Cao, Z. Zhou, C. N. Yang and X. Sun, "Dynamic content selection framework applied to coverless information hiding," *Journal of Internet Technology*, vol. 19, no. 4, pp. 1179–1185, 2018.

[31] Z. Zhou, Y. Mu and Q. M. J. Wu, "Coverless image steganography using partial-duplicate image retrieval," *Soft Computing*, vol. 23, no. 13, pp. 4927–4938, 2019.

[32] Y. Cao, Z. Zhou, Q. M. Jonathan Wu, C. Yuan and X. Sun, "Coverless information hiding based on the generation of anime characters," *EURASIP Journal on Image and Video Processing*, vol. 36, no. 1, pp. 1–15, 2020.