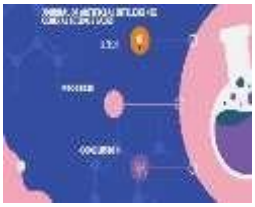
Vol. 5 Issue 01 September, 2024
Journal of Artificial Intelligence General Science JAIGS

Home page https://ojs.boulibrary.com/index.php/JAIGS



Multiple levels of crypto-fiduciary security unforgeable stamp

Edouard Patrick junior onana.

Invention: multy-crypto fiduciary security unforgeable stamp.

Patent WIPO PCT OA2024000001

Copyright DEP638413867013448742

EUIPO 018917917

OAPI 120240056

ARTICLEINFO

Article History:

Received:
01.08.2024
Accepted:
30.08.2024
Online:09 .09.2024

Keyword: Crypto-fiduciary security, unforgeable stamp, cryptographic authentication, tamper-proof seal, blockchain security, data integrity, transaction validation, key management.

ABSTRACT

The paper introduces the concept of a multi-level crypto-fiduciary security system, focusing on the development and implementation of an unforgeable stamp mechanism. This security architecture integrates cryptographic techniques with fiduciary principles to create a robust authentication framework that ensures data integrity, confidentiality, and trust in transactions. The unforgeable stamp serves as a cryptographic seal that is tamper-proof, traceable, and resistant to counterfeiting or duplication, providing enhanced protection against fraud and unauthorized access. The proposed system leverages multiple layers of encryption, key management, and blockchain technology to achieve a secure and verifiable method of transaction validation. This work aims to address critical security challenges in financial, governmental, and other sensitive applications, where trust and data authenticity are paramount.

Multiple levels of crypto-fiduciary security unforgeable stamp.

The present invention relates to a unforgeable seal with multiple levels of crypto-fiat security for securing documents. It is, in fact, a manual stamping device made of wood, without inkwell, ink and ink cassette, combining several levels of cryptographic, fiduciary and biometric security, to authenticate documents. Because of their complexity, they make the documents on which the stamping is affixed forgery-proof.

The particularity of Édouard Patrick Junior Onana's invention is to have created a manual stamp, requiring no energy, equipped with state-of-the-art fiduciary security technologies (anti-copy, anti-scan, complex background, variable optic calligraphy pattern) and digital cryptography technologies. Its combination of cryptographic, fiduciary and biometric methods makes each stamp tamper-proof, ensuring that the stamped document is legitimate. This triple-layer security solution not only eliminates counterfeiting, but also enables real-time document tracking and authentication.

Indeed, the issue of the authentication of documents, of any nature (administrative, financial, judicial, commercial, etc.), is a major concern that is constantly recurrent. This concern is gaining more ground at a time when it is increasingly easy, thanks to computer applications, to modify a text or the stamp that accompanies it.

Not a week goes by without complaints being registered here and there, most of the time relating to the imitation or falsification of the stamping of administrative or judicial documents, with serious legal consequences. Moreover, a close relative suffered for many years of detention, including his family, because of a falsified document.

However, in the traditional way, and until today, the authentication of documents is done with a manual single-color wooden stamp or a personalized or not rubber stamp, and with inkwell. Mono color stamps have security limitations, as the print can easily be scanned and reproduced.

In addition, these stamps, whether made with wood or rubber, can have variations in the quality of the stamping depending on the pressure exerted or the amount of ink applied, which can lead to illegible or inconsistent stampings.

All these limitations of authentication and document security have led us to think about how to solve this problem once and for all.

Technical Market Analysis

On the market, some stamps are pre-inked, which means that they do not need an external inkwell. They are easy to use and provide a crisp, even print. However, some pre-inked ink stamps can be reproduced by creating copies of their stampings by simply scanning or photographing, which can cause problems with the authenticity of the documents. It can be difficult to track the use of pre-inked ink pads, as they do not require frequent refilling. This can make it difficult to manage authorized users and detect abuse.

Another way of stamping is done with digital stamps which are more advanced electronic devices that allow specific texts, patterns or barcodes to be printed on documents. They can be easier to falsify electronically than physical stamps.

Hackers can, in fact, create fraudulent digital stamping using image editing or digital stamp creation software. In addition, digital stamps often store data about the stampings performed. It is important to ensure the security of this data to prevent unauthorized access to this sensitive information.

While digital stamps can stamp electronic documents, it can be difficult to prove the authenticity of these digital documents, as they can be altered or falsified more easily than physical documents.

There are also raised stamps or stamps and dry stamps or stamps or dry stamps which are used to create an embossed print without using ink. However, this feature can be relatively easy to replicate using molding or relief printing techniques, allowing counterfeiters to create counterfeit dry stamps.

In addition, embossed stamps or dry stamps can wear out over time. Which can affect the quality of the stamping and make them less reliable for authenticating the same documents in the long run. While embossed stamps can add a touch of authenticity to documents, they typically do not have complex visual features or built-in security features, making them less effective and more vulnerable in preventing tampering.

Some special inks are used for stamping security documents. They can contain elements such as pigments that are invisible under normal light, but visible under ultraviolet light. Security inks can be tampered with by experienced counterfeiters. Some counterfeiters may be able to reproduce the specific characteristics of security ink, which can compromise the effectiveness of this security measure as well.

Although less common these days, wax seals are used to seal envelopes and official documents. They often have a distinctive seal or pattern. Wax seals can be replicated by creating molds from an original wax seal, making it easy to create counterfeit wax seals.

Wax seals can wear out over time, which can affect the appearance and legibility of the seal, making it difficult to verify its authenticity.

Security stickers typically feature holographic designs, microtexts, or other security features. They may be affixed to documents. In some cases, security stickers can be removed from a genuine product or document and applied to a tampered product or document, which can lead to fraudulent use. Security stickers can be counterfeited by specific individuals or groups. Counterfeiters can create stickers that look similar in appearance to deceive end users.

Digital seals are used for the electronic signature of documents. They offer electronic authentication. Digital seals are stored electronically, making them potentially vulnerable to cyber-attacks. If one of them manages to compromise the digital signing key or security infrastructure, it can put the security of the digital seal at risk.

QR codes can be printed on documents to make it easier to verify their authenticity, using a QR code reader. It is possible to create fake QR codes that look like legitimate QR codes. Users can be tricked into scanning fake QR codes, which can lead to security issues.

As can be seen, all the technical means of securing documents by means of stamping that exist on the market today have limitations and inadequacies and are therefore not immune to imitations and counterfeits. It is these limitations and inadequacies that the present invention called " **multiple levels of crypto-fiduciary security unforgeable stamp** ", corrects.