Hybrid Steganographic Authentication (HSA) – Real-Time Pixel Matching, AI-Driven IDS-SIEM Deep Freeze, and Human-Only Recovery

OPEN ACCESS

Volume: 13

Special Issue: 3

Month: February

Year: 2026

P-ISSN: 2321-788X

E-ISSN: 2582-0397

Citation:
Done, M. S., and K. Sudharsan. "Hybrid Steganographic Authentication (HSA) – Real-Time Pixel Matching, AI-Driven IDS-SIEM Deep Freeze, and Human-Only Recovery." *Shanlax International Journal of Arts, Science and Humanities,* vol. 13, no. 3, 2026, pp. 262–66.

DOI:
https://doiorg/10.34293/sijash.v13iS3-i2-Feb.10287

MS. Done & K. Sudharsan
UG Students, Department of Computer Application
Thiruthangal Nadar College, Chennai

CJ. Manju
Assistant Professor, Department of Computer Application
Thiruthangal Nadar College Chennai

Abstract

This paper presents a new profound way to create a new authentication method that takes really, really long time to crack. Why it takes really, really long time to crack? Unlike traditional method we type password like using special characteristics, even like that, we going to use a new method called image to say. We going to use an image as a password to say. But how you are going to use an image as a password? There's a method in cloud that called PEM or we can call IAM. It's kind of like an authentication but PEM is different. When you upload a file, then only we can access the things in it, like that. So, we going to use an image and upload it so we can use that as a password. What do you mean by uploading an image, can you use it as a password? No. There are additional things that I am adding to it. First, there going to be a cryptographic passkey, a 20 words that we going to use as a password. Well, this is what is going to do. It's going to be the first thing for the password to keep your security. This can be used for companies or like that. For general peoples, you can use without this cryptographic passkey. But it's going to be on higher level, so I am going to show you the cryptographic. This going to be the first. Second, you will upload an image. Third, you will provide a random word. Not a random word, let's say "this is my first time using this authentication." First, there will be a hashed word added to this and randomized and added to the image. Because we are adding a hash, it will be invisible. We cannot see it. Humans cannot see it. Then what happens is the random word that you have given me will be encrypted and added behind the image to say. If you want to understand, let me put it in another way to say. If you're going to take a family photo, on the front of the photo will be the random words with a hash so it cannot be seen. On the back of the image, it will be white, nothing, but the encrypted words will be embedded in the back. So, it will become a three-layered to say. First will be random words, on the second layer will be the image, on the third layer it will be the encrypted words. Because of this, it will be very, very hard time for quantum computing or the current chatbots to crack it. It will take a real long. But to make it even more secure, there is two monitoring and detection system: AI-powered IDS and SIEM. This will constantly monitor. Why? Well, if the quantum computing is like I am going to find certain pixels to say, like that. It will come and find half pixels, then it will come and try again. So, to prevent

this from happening, the AI, which is IDS and SIEM, which is powered by AI, will constantly monitor. Then there's also another thing also, another thing, there must be 75% of the pixels must match immediately. If that doesn't happen, it will trigger Deep Freeze. If this deep Freeze is triggered, it can also be triggered by IDS and SIEM. Well, if this happens, there's only one way to recover, human only recovery method. Well, AI or quantum computing can use forget password and access, but if it's a human recovery, if it cannot be quantum computing, it cannot do anything or neither do AI. Well, how do you recover to say? When this deep-freeze occurs or triggered, there you will be given an opportunity, not an opportunity, you will have to provide your phone number or Gmail to say. After that, there will be a person calling you. If you give a provider a number, the person will call you. Otherwise, you can use the Gmail, you will get a link. You can use an app like Google Meet or anything to face-to-face. They will have certain questions, why did your account got deep Freeze or you have to answer it. That's the only way to recover. Due to this, even quantum computing or anything cannot hack to say every chatbot out there or AI will take really long time to crack and I feel sad for them.

Keywords: Hybrid Steganographic Authentication, Image-Based Authentication, Pixel Matching

Introduction

My name is Done MS, the one who's doing the research paper. I'm not doing it alone. I'm doing it with my best friend Sudarshan K. Well, when I started to do this research, actually there were four members, but midway one of the team members just left. So, what did I do? We three planned to do the first research on cloud. Later, the guy who left came back. So, we split into two teams. We were wondering how to do a research paper, what topic we should pick. My friend said we should not pick a topic, but pick a field. Since all four of us have different interests I'm the communications type who likes multiple fields truth is, I study BCA, but I also have interest in accounts and bioengineering. Sudarshan is my teammate, and I have two other friends, JP and NK. Since NK and JP are doing separate research, Sudarshan and I decided on cybersecurity and quantum computing, but not only for quantum computing for general use. For a week, Sudarshan and I brainstormed. I got an idea: create an authentication method that takes really long to crack. It's like stalling time while it stalls, a monitoring system triggers deep Freeze. I told him, imagine a castle that stalls the enemy until reinforcements arrive. He got it. So, we started. We wondered what to use as a password. I saw a friend who takes selfies, and I thought: let's use a photo as a password. My team agreed. I asked another team about uploading an image for access they mentioned PEM. That's how Image PEM was born. We added AI-powered IDS, SIEM, deep Freeze, and cryptographic passkeys. This method is for both general and quantum-level use. By the end, we felt we had enough cryptographic passkey, Image PEM, random words in front, encrypted words behind, monitored by AI. If pixels don't match, deep Freeze is triggered only human recovery is possible. We thought it's painful for chatbots and AI. We completed half of the research, tried a prototype, and while we needed more resources, it went well.

we understood this password or authentication is really, really strong. So, we thought about making it stronger in the future to say. Well, my friend was a student in Ethical hacking and came to say, he said, there are only two ways to bypass this password to say. Only currently I know these two. One, if you give this password, your password to another and he takes it, that's the one way to crack this password. Second to say, your entire phone gets hacked, then he takes the password. These are the two ways to hack. But he said there are other possibilities to say. Humans are unpredictable than AI, so we have to be vigilant to say. It's true this thing is built like a fortress, but the problem is, even if it's a fortress, there can be people who can bypass the fortress. So, he said to be, the solution case said, be careful, so what can be happened. He's an Ethical Hacking student. I am a student who likes to be in many fields. Commonly, my interest is in BCA and like those technologies. Well, solution is interested in cybersecurity and other things. So, our idea of creating one is something on a common objective.

Methodology

To access and how to use this authentication, first, it will provide you a 20 mnemonic cryptographical word. It's what's mostly used in crypto wallets. If you import it, you can access your crypto wallet. Then you will provide your Gmail. That is for recovery, a default recovery method. Second, why this Gmail is provided: reason is if issues happen in future, to alert you or anything happens. Then next, you have to provide a random word. If you see my abstract, there will be a random—for example, let's say this is the first time I'm using this authentication. This random word—any random word that I've given. It will be randomized and will be kept at the back. You cannot see it. It will be a process that goes on the back. On the third phase, you will provide an image. It can be a family photo, any kind of image that you provided. It can be anything. This image, it will be like that. The process, what will go on the background: the random word that you have given me will be a hash word, will be added in the front. This makes the word invisible, cannot be seen by humans. Certain chatbots neither cannot see that there's an invisible word in the front of the image. This will be added in the front of the image. And the same random word will be randomized a bit and turned into an encrypted word and added at the backside of the image. So, it's like on the first layer, it's going to be the random word, the random hash word, and second, it's going to be the image, on the last, it's going to be the encrypted word. This creates a password to crack because it's using a method called PEM. The PEM method is actually a part of cloud. How it works: you have to upload a file to access it in a particular place, so you can only access it like that. That's how it works. I'm going to use the same thing on image. Because of that, if a quantum computing creates an image, it will have to upload it, and if the image doesn't match, it's going to be a big issue. I will say that on the next step. After that, IDS and SIEM, powered by AI, will activate. It will monitor your account. Then also, it will give you the password into eight clones. Clones means eight will be different, but only you are the one who can know that this is the actual password. Why it gives eight clones: if your phone gets hacked, or say some data has been stolen, these eight clones will be shown. Only one among them is the password. If that person mistakes and uploads that image, that clone, it will trigger deep Freeze. So, it will show this is the password to the user, so you don't need to worry about that. As for deep Freeze, it can be triggered two ways. Well, if you are going to upload the image whenever you are trying to log in, 75% of the pixels must match immediately, or else it will create deep Freeze. That's one. Second, when any suspicious activity is done or goes through your account, it will also trigger a deep freeze. And the only way for you to recover is human-only recovery. Well, to recover that, first you would have provided Gmail. This Gmail will be there, and you can also add another Gmail and also phone number. There will be a video call, or if you are doing that in the Gmail, you can get a link. There is a deep freeze, these kinds of things I have done to recover my account. I need this permission. Google Meet link will be given in Gmail. For phone, there are going to be a call. They will check whether you are human or not, and you have to say the things what happened in detail. After that only, they will let you access your account again, and then you have to create a new password and all things. That's how human-only recovery works.

Background & Related Work

Nowadays, passwords are not strong enough to rely on, and with the rise of new technology like quantum computing, it is becoming easier to crack passwords. People now often rely on passwords or get scammed by others promising, "Give me your account and I'll give it back," but they don't. In cybersecurity, IDS (Intrusion Detection Systems) and SIEMs are not perfect sometimes they produce mishaps, which creates many issues. What my research does is combine authentication and password functions. We can make authentication and password creation simple and straightforward.

HSA (Hybrid Steganographic Authentication) simplifies the process, providing an image format. Even though it uses eight image clones, if just one is mismatched even if your phone is hacked and the hacker chooses the wrong clone out of 8 Deep Freeze will activate, preventing access to the account and securing your data. If we look at today's cybersecurity, even research is sometimes inaccurate, and passwords can be falsified. There are still many problems in IDS and SIEMs. My goal is to create a simple yet tough authentication system one that takes a very long time to crack. In that time, IDS will properly detect issues and alert the user. If IDS fails, pixel matching ensures that if 75% of pixels don't match instantly, Deep Freeze triggers. This is beneficial because IDS and SIEM don't have to overwork. As for related works, I drew inspiration from other researchers, such as the Hybrid Framework, though I'm not sure of the team's name.

Our work took around one to three months to complete. Some related concepts come from cloud technologies like PAM but we had to create a new method, Image PEM. This is also a new innovation. Additionally, the reason we chose a long-time-to-crack password is that, given the cost of RAM and computing resources, cracking it would require significant effort. It would simply be too costly and take a very long time, making it a waste of resources to attempt cracking a password or authentication system like this.

Conclusion

Nowadays, passwords are not strong enough. Even if, for example, you forget a password, you can use email to recover it. But if someone has access to that same email, they can use it to get the password. Just like my friend who lost his gaming account and Gmail he still hasn't recovered them. Since this method uses human-only recovery, that will be easier. Compared to traditional passwords, recovery will be quick and face-to-face. So, AI and quantum computing can do nothing about it. Another thing: there is a Deep Freeze mechanism. This Deep Freeze mechanism will stop any output from being taken, and no one can access your account. The only way is bypassing it, which would create a big issue. Since you cannot access the account, someone else might try to get your password, triggering Deep Freeze. No one can lay a hand on your data that you're trying to keep safe. That is a plus compared to traditional passwords like OTP and other current methods. Even with OTP, if someone gets it, they can log in easily. No one can stop that. What my HSA in my research paper will do is prevent these things, since there is no OTP. If something suspicious is going on, IDS will trigger, and SIEMs will trigger Deep Freeze. These two things will stop it. If 75% of the image matches immediately, there will be eight clones in the authentication, and only one is the real password. If your mobile gets hacked, it will be confusing because you need to know which one is real. That's how our method breaks down and keeps it simple. An image is something we all have. Even if someone doesn't take many photos, they will have some family, themselves, or places they love. If 70% of people have phones, and each has two or three photos, there will be more images than the population. Even if content matching tries to use these images, it will take a long time because there are so many. It will be very, very time-consuming. This is not cost-effective because it consumes a lot of time and resources. Cracking a password like this is not worth it. Even if AI tries, it's not cost-effective. They would rather use a backdoor. That's what this prevents. As for future work, to make it even stronger, we plan to take the image, divide it into 9x9 blocks, shuffle, and re-merge. Or, for more security, 4x4, 5x5, 6x6, 9x9, 10x10 cut, re-merge, cut again. It will become a jumble. Since a human might not always be there to recover, we plan an alternative recovery method. That's our future plan. Compared to another authentication, this can bypass quantum computing today, making it very hard to crack. I think there are only two ways to crack it: One, you give your password to someone, and they cheat you. But you cannot use "forgot password" because you can use your mobile to free your account and recover.

References

Books

1. Wittig, A., & Wittig, R. (2016). Amazon Web Services in Action. Manning Publications. Covers secure image handling and steganography patterns in cloud storage.
2. Gregg, B. (2020). Systems Performance: Enterprise and the Cloud. Addison-Wesley. Explains real-time pixel-matching latency and AI-driven monitoring.

Journal Articles

3. Baseline for IDS-SIEM in IoT-like auth flows.
4. Ghazaryan, E. (2025). "Comparative Analysis of Cloud Deployment Models." International Journal of Engineering and Computer Science, Article ID 5193. Multi-layer image encryption trade-offs.
5. Lee, G., Chun, B.-G., & Katz, R. H. (2010). "Topology-Aware Resource Allocation for Data-Intensive Applications in Cloud." ACM SIGCOMM Computer Communication Review, 40(5), 120-126. Pixel checksum routing ideas.
6. Kleppmann, M. (2017). "Designing Data-Intensive Applications." O'Reilly Media, pp. 1-600. LSB stego persistence under compression.

Conference Papers

7. Villegas, D., Antoniou, A., & Sadjadi, S. M. (2010). "Security and Performance Trade-off in PerfCloud." VHPC Workshop at SC Conference, pp. 1-10. Human intervention as last gate.
8. Pate, S. (2021). "Learning AWS: Design, Build, and Deploy Responsive Applications." Packt Publishing Conference Proceedings, pp. 1-400. IoT-inspired pixel verification.