Issue Brief

August 2026
No: 539

Beyond the Password: The Evolution of Identity Verification and the Mounting Challenge of Biometric Security in Military Environments

Lt Col Jagmit Singh
Brig Deven Makhija
Dr Hemprasad Yashwant Patil
Dr Somnath Dey

Beyond the Password: The Evolution of Identity Verification and the Mounting Challenge of Biometric Security in Military Environments

Abstract

For a long time, the method of challenging by asking a question, "Stop! Who comes here?" has been central to any military unit/station. In the present scenario, the question still remains the same but the way of answering has changed over time— from spoken passwords at the gate to identity cards, PINs and now automated facial recognition. However, with the advancement of technology, 'these secure means' has been challenged.

This issue brief traces development— from the sentry's simple challenge to the biometric systems being used today. It also argues that passwords and single factor authentication are no longer enough for secure systems as biometric systems which were once seen as a major advance, now faces new threats from deepfakes and AI-generated faces.

Keywords: Biometric Security, Defence Requirement, Encryption, Secured Database, Cyber

Introduction

For a long time, military commanders have faced the same basic problem of identification of the person entering the secure access areas. If a wrong access is made, it will make the whole system vulnerable. A spy, an intruder or someone using a false identity can cause serious harm to the data, sensitive information and artefacts. These are real threats with serious security risks. Over time, the way militaries check identity has changed a great deal because of new technology, larger systems and smarter attackers. What has stayed the same is the struggle between the person trying to prove their identity and the person trying to fake it. This article looks at how identity checks have changed, what the weaknesses of each method are and what strong verification should look like today, especially now that fake faces can be created with simple technology.

Password: The Original Shared Secret

The simplest form of identity verification is the shared secret. Both parties viz. the sentry and the approaching soldier, who knows a word or phrase that has been agreed in advance. Knowledge of that word is taken as proof of belonging. Roman legions used this

system. Medieval fortresses used it. It was standard practice in every army through the Second World War, where the daily 'challenge and password' was a routine feature of military life.

The appeal of the password is its simplicity. It requires no technology, no equipment and no bureaucracy beyond the distribution of the word at the start of the day. In a world wherein the number of people who needed to prove their identity was small and the time available to forge a false identity was long, it worked reasonably well.

Its weaknesses, however are structural and cannot be engineered away. A shared secret that is known to many people is, inevitably, not a secret anymore.. It can be overheard, extracted under duress or simply told to the wrong person. In the Second World War, German infiltrators, during the Battle of the Bulge, reportedly used their knowledge of American passwords (Morse Code) obtained through captured soldiers to pass allied checkpoints which was a vivid illustration of the password's fundamental fragility. Once the secret is out, every gate it protects is open.

The deeper problem is that, a password verifies knowledge, not identity. It shows the sentry that the person at the gate knows the password, but it does not prove who that person really is. In a small unit where everyone knows one another, that difference may not seem important. In a large organisation with hundreds of personnel and regular turnover, it matters enormously.

The Identity Card: Adding the Visual Check

As military organisations grew in scale and complexity through the twentieth century, the password alone became clearly insufficient. The response was an identity document, initially a simple paper card with a photograph and personal details, later a laminated card with more sophisticated printing and eventually a card embedded with digital information and a machine-readable chip.

The identity card introduced a significant conceptual advance: it linked the claim of identity to a physical token that was harder to produce than a spoken word and that carried visual information like a photograph that could be compared against the holder. For the first time, the sentry had something to look at as well as something to hear.

Yet the card system introduced its own vulnerabilities and they followed a familiar pattern. The value of an identity card depends entirely on the difficulty of producing a false

one. When that difficulty is high, then the card is printed on specialised paper with security inks and holograms then forgery is limited to well-resourced adversaries. As printing improved and became easy to access, it also became easier to make fake documents that looked real. By the 1990s, desktop printing and lamination had advanced enough that even well-made fake ID cards were no longer limited to powerful groups.

A photo on an ID card has its own weakness. It only works if a person can compare the face on the card with the person standing in front of them and that is not always easy. Poor lighting, time pressure, a changed appearance or a misleading resemblance can all lead to mistakes.

The Digital Age: PINs, Passwords, and the Problem of Scale

The computerisation of defence systems from 1970s onwards introduced a new category of access control challenge. It was no longer sufficient to verify who was entering a physical space; it became necessary to verify who was logging into a computer system, authorising a transaction or accessing a classified database. The solution that emerged was the Personal Identification Number, or PIN, and the digital password which was in conceptual terms identical to the spoken password of the Roman sentry. It was a shared secret, now memorised as a number or a string of characters rather than a word.

Digital passwords offered some advantages over their spoken predecessors. They could be changed frequently. They could be required to meet complexity standards. They could be stored in encrypted form so that even an insider who accessed the storage system could not easily read them. And a failed attempt could trigger a lockout, thus limiting the value of trying combinations at random.

In practice, however, the digital password has proven chronically difficult to manage at the scale of a large organisation. People choose weak passwords like words, names, dates because strong ones are hard to remember. They write them down. They reuse the same password across multiple systems. They share them with colleagues for convenience. In study after study of corporate and government security breaches, compromised or weak passwords have featured as a primary or contributing cause. The military is not immune to this problem either. A password only shows that a person knows the secret— it does not prove their true identity. If an attacker learns the password through deception, a data breach, observation or by

forcing someone to reveal it, the protection is lost. And unlike a physical key, a password leaves no physical trace of having been taken. The holder may not know their credential has been compromised until it is used against them.

Biometrics: Verifying What You Are, Not What You Know

The insight that drove the adoption of biometric verification was straightforward: rather than asking 'What do you know?' or 'What do you have?', ask 'What are you?' A person's fingerprints, the pattern of their iris, the geometry of their face or the sound of their voice are properties that cannot be forgotten, lost or easily transferred. They are, in principle, intrinsic to the individual in a way that passwords and cards are not.

Automated fingerprint recognition became the first widely deployed biometric technology, used for criminal identification from the late nineteenth century and adopted into military and government identity systems from the 1990s onwards. Iris recognition, which exploits the unique random pattern of the iris formed in early infancy and stable throughout life, followed as an even more accurate biometric. Facial recognition which is the automated comparison of a camera image against a reference photograph emerged as perhaps the most practically appealing biometric for access control, since it requires no physical contact and no deliberate action on the part of the person being identified.

The adoption of facial recognition, in particular, has accelerated sharply with advances in machine learning. Modern facial recognition systems can identify individuals from a camera image with accuracy that, under controlled conditions, substantially exceeds that of an unaided human reviewer. They work all the time on their own, without needing a sentry to make a quick decision under pressure. For a military organisation that has to control access to hundreds of places across a large base, this is a very practical advantage.

Biometrics seemed to fix the main weakness of password-based checks. A biometric cannot be forgotten or guessed, and it is much harder to pass on to someone else than a card or a password. For a while, it seemed that identity verification had finally moved in the defender's favour.

The New Threat: When Faces Can Be Fabricated

The optimism that accompanied early biometric deployment has been substantially revised by developments in artificial intelligence over the past decade. The specific

development that bears most directly on facial recognition is the emergence of generative AI systems capable of producing synthetic images and videos that are, to a camera and to the naked eye, indistinguishable from genuine ones.

The technology behind this capability is generative adversarial networks and more recently, diffusion-based image synthesis which works by training a computer model on large numbers of genuine photographs until the model learns the statistical patterns that make a face look real. It can then generate new faces that have never existed, or impose the appearance of a known person's face onto a different person's video— the technique commonly known as Deep Fake. The results, at the current state of the art, are of a quality that fools human observers a substantial proportion of the time and that can deceive a facial recognition system that is looking only at the image and not at additional signals.

For a military access control system, this represents a qualitative shift in threat. An adversary who wishes to impersonate a specific authorised individual no longer needs to physically resemble that person, steal their card or extract their password. They need a sufficient number of photographs of that individual like the kind of photographs that appear in publicly available sources for a great many defence personnel and access to generative AI software that is freely available online. It is now much easier to fake a biometric identity than it was earlier. This is important because militaries now rely more and more on automated systems to verify identity before giving someone access or permission to act. In that situation, a weak check is not just a weak gate. It can compromise the whole security system.

What Robust Verification Looks Like: The Principle of Layered Evidence

is the changing security pattern is quiet clear— when security relies on only one check, it is likely to be defeated if an attacker gets through a weakest and vulnerable point like passwords can be stolen, ID cards can be forged, PINs can be guessed or tricked out of people and facial recognition can now be fooled with fake images or replay attacks. This shows that while one technology is good but, it may eventually fail.

The measures to counter the failure is to use several independent checks and methods together. This is the key idea behind multi-factor authentication which combines PIN, card or token and multi-modal biometrics. For facial recognition, it is like checking more than just the face in a flat image. The system can also look at depth, gaze and eye movement for

identification as a full proof measure. For example, a replayed video may fail the depth check, a fake face may pass the depth test but fail the gaze test and a mask may still fail the eye-movement check. No single check is perfect, but using multiple together makes it much harder to bypass the system.

Challenges for Military Establishments

The practical implementation of these measures has many challenges as mentioned below:

- Many defence systems still uses a mix of old and new access methods, with stronger biometric systems at important access areas and older card or PIN-based systems at less critical ones. It is not realistic and feasible to replace everything at once, hence, during transition the attacker may easily target the weakest point viz. often the oldest system to compromise the security.
- The Security problem is dynamic and ever evolving like a moving target. As better liveness checks come online, attackers will study them and hunt for ways to bypass them. The same cycle has played out with every earlier identity system. Defence organisations therefore need to keep improving their systems over time rather than treating security as a one-time upgrade.
- Human behaviour is also an important parameter which defines the security of any system. Even the most advanced technical system can be compromised if people share credentials, choose weak passwords or fall for social engineering. Technical safeguards and security awareness among personnel —both have to be in place and both need to improve over time.
- Securing biometric data is equally an important challenge. Fingerprints and face images are very sensitive and if they are stolen, the damage can be much harder to fix than a password leak. A password can be changed, but a face cannot. Protecting biometric databases demands the same level of security as the access control systems they support.
- In field environments like forward operating bases, mobile command posts, border outposts wherein controlled conditions under which biometric systems perform optimally may not always obtain. Lighting, weather, equipment wear and operational tempo all affects system reliability. Robust verification architecture must account for the conditions of actual deployment, and not just laboratory testing.

Way Forward

Several priorities follow from the analysis above.

- High-priority access points like the command facilities, communication centres, armoured vehicle control systems and stores of sensitive material should be subject to an immediate review of their verification architecture, with a view to identifying those that relies on a single factor and are therefore most exposed to the current generation of spoofing threats.
- Procurement standards for new biometric access control systems should specify layered verification as a minimum requirement, rather than treating it as an optional enhancement. A system that checks only a face, without any liveness check, is not enough to stop a skilled attacker in 2026.
- Military training should also include new threats like deepfakes in simple terms— how they are made and why they can create real risks for military operations. Personnels now understands that, threat are better placed to apply appropriate scepticism in contexts wherein identity cannot be automatically verified.
- India's existing defence AI systems , frameworks and the iDEX ecosystem should be used to support the development of advanced biometric systems indigenously. This would reduce dependence on foreign suppliers for a technology that is central to both physical security and operational security.
- Regular adversarial testing of deployed systems using the same techniques that a real adversary might employ should be incorporated into the standard cycle of security audits, ensuring that the gap between what a system was designed to defeat and what it can actually defeat in practice is identified and addressed before an adversary exploits it.

Conclusion

The question 'Who comes here?' is as old as the organised military. The tools used to answer it have changed beyond recognition— from the spoken word in the dark to the neural network comparing a camera image against a database; however, the underlying contest between the verifier and the impostor has remained constant. History shows, with

uncomfortable regularity, that every verification system that relies on a single layer of evidence is eventually defeated by an adversary patient and resourceful enough to attack that layer.

The current generation of AI-driven synthetic imagery represents a specific and serious attack on facial biometric verification, the technology in which militaries and security establishments have placed increasing trust over the past two decades. The response is not to abandon biometric verification, which offers genuine advantages over knowledge-based and token-based systems, but to layer it with additional checks that an adversary cannot simultaneously defeat. This is not a distant aspiration; the technical means to do so exists today.

What is required is the institutional will to treat robust identity verification as a frontline security priority rather than an administrative function and to invest in it with same seriousness that defence establishments apply to the more visible dimensions of security. The soldier who once stood at the gate knew that a 'wrong answer delivering person could be a foe'. That same understanding needs to be carried forward into the architecture of the digital gatekeepers which do the soldier job's in the present scenario of technological advancement.

Works Cited

Caldwell, M., Andrews, J. T. A., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. Crime Science, 9(1), 14. https://doi.org/10.1186/s40163-020-00123-8.

Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Profile Books.

Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. (2020). Deepfakes and beyond: A survey of face manipulation and fake detection. *Information Fusion*, 64, 131–148. https://doi.org/10.1016/j.inffus.2020.06.014.

Turland, J., Coventry, L., Jeske, D., Coventry, P., & van der Linden, S. (2015). Nudging towards security: Developing an application for tailoring security advice. In Proceedings of the British HCI Conference 2015 (pp. 1–9). BCS. https://doi.org/10.14236/ewic/HCI2015.19.

Zhang, Z., Yan, J., Liu, S., Lei, Z., Yi, D., & Li, S. Z. (2012). A face anti-spoofing database with diverse attacks. In Proceedings of the 5th IAPR International Conference on Biometrics (ICB) (pp. 26–31). IEEE. https://doi.org/10.1109/ICB.2012.6199754.

About the Author

Lieutenant Colonel Jagmit Singh is an Infantry Officer with a keen interest in artificial intelligence and machine learning. The officer is actively engaged in AI research projects, focusing on practical applications in security and defence. He has the experience of serving in Northern and Eastern parts and is utilising his operational experience with technical curiosity to explore innovative solutions that enhance modern warfare capabilities.

Brigadier Deven Makhija is a senior officer and researcher and academic with expertise in artificial intelligence, machine learning, cybersecurity and defence technologies. His research focuses on the application of intelligent systems to secure, resilient, and mission-critical technologies, with contributions spanning AI-driven decision support, communication systems, and advanced defence applications.

Dr Hemprasad Yashwant Patil is currently serving as an Associate Professor at the Military College of Telecommunication Engineering, Mhow, India. His primary re-search interests include Cyber Security, Artificial Intelligence, Data Science and Agentic Autonomous Systems.

Dr. Somnath Dey is currently working as a Professor in the Department of Computer Science Engineering at the Indian Institute of Technology Indore (IIT Indore). He has published over 40 research articles (including papers in international journals, conferences and book chapters). He is actively involved in academic and industrial collaboration for research and development.